Statement: Age Assurance and Children's Access

Statement

Published 16 January 2025

Contents

Section

Annex

1. Overview

What we are doing today

Robust age checks are a cornerstone of the Online Safety Act. Our decisions today on age assurance are the next step in implementing the Act and creating a safer life online for people in the UK, particularly children. This follows the publication of our Illegal Harms Codes and guidance in December 2024.

The research and evidence we have collected during our consultations show that children online in the UK have access to a wide range of content that is harmful to them. This includes pornographic content, content that promotes suicide, self-harm and eating disorders, and other content which is harmful to children.

From today, all user-to-user and search services have three months to assess whether they are likely to be accessed by children. Once our Protection of Children Codes and guidance are finalised in April 2025, platforms likely to be used by children will need to assess the risks they pose and take action to protect them – which may include using highly effective age assurance to prevent them from accessing harmful content.

All service providers which allow pornography must implement highly effective age assurance to ensure that children are not normally able to encounter pornographic content.

The Online Safety Act is being implemented in phases. We expect the approach to highly effective age assurance that we are setting out today to apply to all parts of the online safety regime. This gives providers certainty about what action they need to take to meet our rules.

What will change

This statement, together with our Protection of Children Codes and guidance which we will publish in April 2025, will deliver a step change in the experience of children online through an ambitious set of protections:

- **Children's access assessments:** all user-to-user and search services in scope of the Act must conduct a children's access assessment to establish if their service or part of it is likely to be accessed by children. **From today**, these services have three months (**by 16 April 2025 at the latest**) to complete their children's access assessment. Unless they are already using highly effective age assurance, we anticipate that most of these services will need to conclude that they are likely to be accessed by children within the meaning of the Act. Under the Act, services likely to be accessed by children must comply with the children's risk assessment duties and the children's safety duties.
- **Measures to protect children:** we will publish our Protection of Children Codes and children's risk assessment guidance (along with other guidance) in April 2025. This will mean that services that are likely to be accessed by children will need to conduct a children's risk assessment **by July 2025** – that is, within three months. Following this, they will need to implement measures to protect children on their services in line with our Protection of Children Codes to address the risks of harm identified. These measures may include

introducing age assurance to prevent child users from accessing their platform and/or protect them from harmful content.

- **Services that allow pornography:** all services which allow pornography must have highly effective age assurance in place **by July 2025 at the latest** to prevent children from accessing it. The Act imposes different deadlines on different types of provider. Services that display or publish their own pornographic content, including certain Generative AI tools, **must begin taking steps immediately** to introduce robust age checks. Services that host user-generated pornographic content must have fully implemented age checks by July.

What does highly effective age assurance mean

Today we set out our conclusions on what we consider to be 'highly effective age assurance'. Our approach is designed to be flexible, tech-neutral and future-proof, with the protection of children at its heart. In our approach to highly effective age assurance we have:

- Confirmed the criteria that age assurance methods must meet to be considered highly effective: they should be technically accurate, robust, reliable and fair;
- Set out a non-exhaustive list of age assurance methods that we consider are capable of being highly effective, including mobile network operator age checks, credit card checks, digital identity services and certain age estimation methods;
- Confirmed that less effective methods of age assurance – including self-declaration of age and online payments which do not require a person to be 18 – are not compliant with the requirement to have highly effective age assurance;
- Stipulated that harmful content must not be visible to users before, or during, the process of completing an age check;
- Made clear that services should not host or permit content that directs or encourages children to attempt to circumvent age and access controls[1]; and
- Set expectations that services consider the interests of all users when implementing age assurance – affording strong protection to children, while taking care that privacy rights are respected.

Next steps

We expect all providers to take a proactive approach to compliance and meet the deadlines set out above. Ofcom is today opening an enforcement programme to monitor and assess compliance with the requirements to implement highly effective age assurance on services that allow pornographic content. We will first focus on services that publish their own pornographic content, extending the programme to include all relevant services as soon as the broader children's safety duties come into effect.

[1] We use the term "access controls" to describe a technical mechanism(s) which prevents users who have not been age assured, or having been age assured, did not meet the requirements of the age assurance process, from accessing a service (or part of it) or certain content.

We will contact a wide range of adult services – large and small – to advise them of their new obligations and monitor their compliance. We will not hesitate to take enforcement action against services that do not comply.

As set out in our updated roadmap,[2] following the publication of our Illegal Harms Codes in December, the second phase of our implementation of the Act is now underway. Future milestones include:

- **February 2025:** Consultation on draft Guidance on wider protections for women and girls;
- **April 2025:** Protection of Children statement, including final Protection of Children Codes and guidance, following our Consultation in May 2024; and
- **Spring 2025:** Consultation on additional Codes of Practice measures, including proposals on extending the role of highly effective age assurance to protect children from grooming.

Phase three will establish additional requirements for categorised services, focused on bringing an enhanced level of safety, transparency, and accountability to some of the largest service providers operating in the online world. With the categorisation thresholds now published,[3] we expect to deliver this work to the following timeline:

- **Summer 2025:** Publish the register of categorised services;
- **Summer 2025:** Issue draft and final transparency notices to categorised services; and
- **Early 2026:** Publish draft proposals regarding additional duties on categorised services. Based on our experience of large regulatory publications, our current planning assumption is to issue the statement around one year after consultation.

[2] Ofcom, 2024, Ofcom's approach to implementing the Online Safety Act - Ofcom.
[3] The draft Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025

2. Introduction, our duties, and navigating the statement

- This section provides a high-level introduction to our statement. We summarise our key relevant duties and functions, explain what is covered in the statement and set out next steps.

What this section does

2.1 This section provides an overview of some of our key relevant duties and functions.[4] This section also explains what is covered in this statement and sets out next steps.

2.2 We call our decision documents 'statements' because they are statements of our reasoning for the decisions we have made. This statement is the first step in putting into effect the new online safety regulatory regime for the protection of children, established by the Online Safety Act 2023 ("the Act").

Overview of the legal framework

Ofcom's general duties

2.3 Ofcom is the independent regulator for communications services. We have regulatory responsibilities for the telecommunications, post and broadcasting sectors, as well as for online services. These include U2U, search and pornography services regulated under the Act, as well as online video services, such as on-demand programme services and video-sharing platforms ("VSPs") established in the UK.[5]

2.4 As a public authority, Ofcom must act lawfully, rationally and fairly.

2.5 The Communications Act 2003 ("the 2003 Act") places a number of duties on us that we must fulfil when exercising our regulatory functions, including our online safety functions. The 2003 Act states that our principal duty in carrying out our functions is:

- to further the interests of citizens in relation to communication matters; and
- to further the interests of consumers in relevant markets, where appropriate by promoting competition.[6]

[4] The legal framework is set out in greater detail in Annex 1.
[5] For more detail about the nature of these regulated services, see Overview of regulated services from our December 2024 statement Protecting people from illegal harms online.
[6] Section 3(1) of the 2003 Act.

2.6 In performing that principal duty, we must have regard to principles set out in the 2003 Act, which says that regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed.[7]

2.7 In carrying out our functions, Ofcom is required to secure, in particular, adequate protection of citizens from harm presented by content on regulated services, through providers using appropriate systems and processes designed to reduce the risk of harm.[8]

2.8 The 2003 Act further requires[9] that we must have regard to the following as they appear to us to be relevant in the circumstances. In making our decisions, we have considered factors including, but not limited to:

- the risk of harm to citizens presented by regulated services;
- the need for a higher level of protection for children than for adults;
- the need for it to be clear to providers of regulated services how they may comply with their duties under the Act;
- the need to exercise our functions to secure that providers may comply with such duties by taking or using measures, systems or processes which are proportionate to the size or capacity of the provider and the level of risk (and potential severity) of harm presented by the service;
- the desirability of promoting the use of technologies which are designed to reduce the risk of harm to citizens; and
- the extent to which providers demonstrate, in a way that is transparent and accountable, that they are complying with their duties.

2.9 In line with our additional duties under the 2003 Act,[10] we have also considered the vulnerability of children and of others whose circumstances put them in need of special protection. We have considered:

- the desirability of promoting competition and encouraging investment and innovation in relevant markets;
- the needs of persons with disabilities, the elderly, and of those on low incomes;
- the opinions of consumers and of members of the public generally;
- the interests of persons in the different parts of the United Kingdom; and
- the interests of the different ethnic communities within the United Kingdom.

Children's safety under the Online Safety Act

2.10 The Act provides for a new regulatory framework which has the general purpose of making the use of regulated internet services safer for individuals in the UK. Securing better protections for children so that they are safer online is one of the core objectives of the Act. The Act is clear that the duties imposed on regulated services seek to secure (among other

[7] We must also have regard to any other principles appearing to us to represent best regulatory practice.
[8] Section 3(2)(g) of the 2003 Act (as amended by section 91 of the Act).
[9] Section 3(4A) of the 2003 Act.
[10] Section 3(4) of the 2003 Act.

things) that regulated services are safe by design, and designed and operated in a way that a higher standard of protection is provided for children than for adults.[11]

2.11 Part 3 of the Act places duties on providers of regulated U2U services and providers of regulated search services to identify, mitigate and manage the risks of harm from illegal content and activity and content and activity that is harmful to children. We refer to these services as "Part 3 services". These duties include a duty to carry out children's access assessments in order to determine whether the service is "likely to be accessed by children".[12] Part 3 services that are "likely to be accessed by children" are subject to duties relating to the protection of children from content that is legal but is harmful to them (known as "content that is harmful to children"[13]).[14] We explain these duties in more detail in Annex 1.

2.12 Part 5 of the Act imposes specific duties on service providers that display or publish pornographic content on their online services. We refer to these services as "Part 5 services". These include the duty to implement age assurance to ensure that children are not normally able to encounter such content and duties relating to record keeping.[15] The age assurance must be implemented and used in a way that is highly effective at correctly determining whether or not a user is a child. We explain these duties in more detail in Annex 1.

2.13 The Act also imposes duties on Ofcom to:

- Produce guidance for providers of Part 3 services to assist them in complying with their duties in relation to children's access assessments.[16]
- Prepare and issue Codes of Practice – these are a package of measures recommended for service providers to comply with their safety duties under the Act, including the duties on Part 3 services likely to be accessed by children relating to the protection of children.[17] In preparing Codes of Practice, Ofcom must have regard to the principles and objectives set out in Schedule 4 to the Act.[18]
- Produce guidance for providers of Part 5 services to assist them in complying with the age assurance and record keeping duties.[19]

[11] Section 1 of the Act. This is also reflected in the duties imposed on Ofcom under the Act, including the duty on Ofcom to have regard when performing our online safety functions to the need for a higher level of protection for children than for adults (s3(4A)(b)).
[12] Sections 35-37 of the Act.
[13] As defined in section 60 of the Act.
[14] As set out in sections 11-13 and 20-21 for regulated U2U services and sections 28-30 and 31-32 for regulated search services.
[15] Section 81 of the Act.
[16] Section 52(3)(b) of the Act.
[17] Section 41 of the Act.
[18] As explained below, we are not reaching any final decisions on Ofcom's Protection of Children Codes in this statement and will do so in our April statement. However, we have set out in Annex 1 the relevant provisions in Schedule 4 for completeness.
[19] Section 82 of the Act.

Impact assessment

2.14 Impact assessments provide a valuable way of evaluating the options for regulation and showing why the chosen option(s) was preferred. They form part of best practice policy making. This is reflected in section 7 of the 2003 Act, which requires Ofcom to carry out and publish an assessment of the likely impact of implementing a proposal which would be likely to have a significant impact on businesses or the general public, or when there is a major change in Ofcom's activities. As a matter of policy, Ofcom is committed to carrying out impact assessments in a large majority of our policy decisions. Our impact assessment guidance sets out our general approach to how we assess and present the impact of our proposed decisions. We discuss our impact assessments on measures covered by this statement in Annex 2.

Human rights

2.15 It is unlawful for Ofcom to act in a way which is incompatible with the European Convention on Human Rights ("ECHR").[20]

2.16 Of particular relevance to Ofcom's functions under the Act are the right to freedom of expression (Article 10 ECHR) and the right to privacy (Article 8 ECHR). Other ECHR rights which may also be relevant to Ofcom's functions under the Act are the right to freedom of thought, conscience and religion (Article 9 ECHR) and the right to freedom of assembly and association (Article 11 ECHR). In formulating our decisions in this statement, we have carefully analysed where we have identified the potential for interference with ECHR rights, to make sure any such interference is proportionate. This analysis is also set out in Annex 2.

Equality and Welsh language impact assessments

2.17 We have considered the equality impacts of the guidance set out in this statement, detailing our understanding of any particular impacts on protected groups in the UK.

2.18 Where relevant and to the extent we have discretion to do so in the exercise of our functions, we have considered the potential impacts on opportunities to use the Welsh language and the need to treat the Welsh language no less favourably than English (in accordance with Welsh language standards).

2.19 We have included our considerations on those specific impacts in Annex 2.

[20] Section 7 of the 2003 Act, as amended by section 93 of the Act.

What we cover in this statement

2.20 The decisions explained in this statement set out our final positions on highly effective age assurance ("HEAA") and what this means for the three pieces of guidance for industry which we are publishing today under the Act: our Guidance for service providers publishing pornographic content ("Part 5 Guidance"), our Guidance for Part 3 services on highly effective age assurance ("Part 3 HEAA Guidance") and our Children's Access Assessments Guidance.

2.21 In reaching our final positions, we have considered responses to our December 2023 consultation, Guidance for service providers publishing pornographic content ("December 2023 Part 5 Consultation"),[21] together with responses to our May 2024 consultation Protecting Children from Harms Online ("May 2024 Consultation")[22] that related to our overall approach to highly effective age assurance and our approach to children's access assessments. Our expectations regarding the standard of highly effective age assurance are consistent across Part 5 and Part 3 of the Act.

2.22 This statement does not consider stakeholder feedback on the proposed age assurance measures in the draft Protection of Children Code of Practice ("Protection of Children Codes") for user-to-user services, which we published alongside our May 2024 Consultation.[23] Our summary and consideration of these responses will be set out in our Protection of Children Statement in April 2025.[24]

2.23 We are broadly confirming the proposed approach that we set out in our December 2023 and May 2024 consultations, which we consider will secure the best outcomes for the protection of children online in the early years of the regime. In order for their age assurance process to be highly effective, service providers need to meet four criteria: technical accuracy, robustness, reliability and fairness. We recognise that there are a number of different age assurance methods which are capable of being highly effective and we have deliberately taken a flexible, tech-neutral, future-proofed approach. Service providers should also consider the principles of accessibility and interoperability. We are also clear that, in implementing a highly effective age assurance process, services are also bound by data protection laws. Compliance by service providers with both the online safety and the data protection regime is mandatory and should not be considered a trade-off. We have set out a non-exhaustive list of kinds of age assurance which could be capable of being highly effective, but it is the responsibility of service providers to assess for themselves whether their age assurance process meets our four criteria. We do not consider that it would be appropriate to introduce numerical thresholds at this time to support the criteria as an indicator of compliance. However, we may do so in future, pending further

[21] Ofcom, 2023, Consultation: Guidance for service providers publishing pornographic content
[22] Ofcom, 2024, Consultation: Protecting children from harms online - Ofcom
[23] Ofcom, 2024, Protection of Children Code of Practice for user-to-user services. We referred to the draft Protection of Children Codes of Practice as the draft 'Children's Safety Codes' in our May 2024 Consultation.
[24] In April 2025 when we publish our Protection of Children Statement, we will update our Part 3 HEAA Guidance with references to the final Protection of Children Codes and Children's Risk Assessment Guidance as appropriate, including to reflect any changes to the wording of the relevant Codes measures. Beyond April 2025, we may update the guidance where necessary to reflect any future age assurance measures.

developments in testing methodology, industry standards, and independent evidence on the performance and capabilities of different age assurance methods.

2.24 The Act makes a distinction between different types of adult services, which impacts on the timing of implementation of highly effective assurance. Part 5 services must implement age checks immediately. User-to-user services that allow pornographic content will be required to implement age assurance measures from July, when we expect the children's safety duties to come into force following the publication of our Protection of Children Codes.[25] It is for services themselves to assess whether the content on their sites falls into Part 5 or Part 3 and take the necessary steps to meet their obligations.

2.25 In terms of the structure of this statement:

- In Section 3, we set out our final position on our approach to highly effective age assurance for Part 3 and Part 5 services, including our reasoning and response to views contributed by respondents. This HEAA approach is reflected in both our Part 5 Guidance and Part 3 HEAA Guidance.
- In Section 4, we set out our final position on other considerations specific to the Part 5 Guidance, beyond the duty to ensure that age assurance is highly effective at correctly determining whether a user is a child. This includes guidance on the scope of Part 5, record keeping, and our approach to enforcement of the Part 5 duties.
- In Section 5, we set out our final position on children's access assessments. This section sets out the two stages of the children's access assessment. For stage 1, it explains our approach to how services can determine whether it is possible for children to access their service. This includes reference to whether services have age assurance in place which would meet the criteria in Section 3 and therefore be able to be considered highly effective. For stage 2, this section explains our decision and reasoning to provide criteria and examples for services to assess whether they meet the child user condition (which determines whether children are likely to access their service).
- Annex 1 sets out our legal framework.
- Annex 2 sets out our approach to impact assessments, which include our impact assessment for our approach to highly effective age assurance and other elements of the Part 5 Guidance, our impact assessment for our approach to children's access assessments, together with our specific equality and Welsh language impact assessments as well as rights assessments.
- In Annex 3, we set out the evidence we drew on to compile the list of factors to consider for children's access assessments. We originally set out this evidence at Section 5 of our May 2024 Consultation and have updated sources where more recent findings are now available.
- Annex 4 includes our glossary of terms used in this statement.

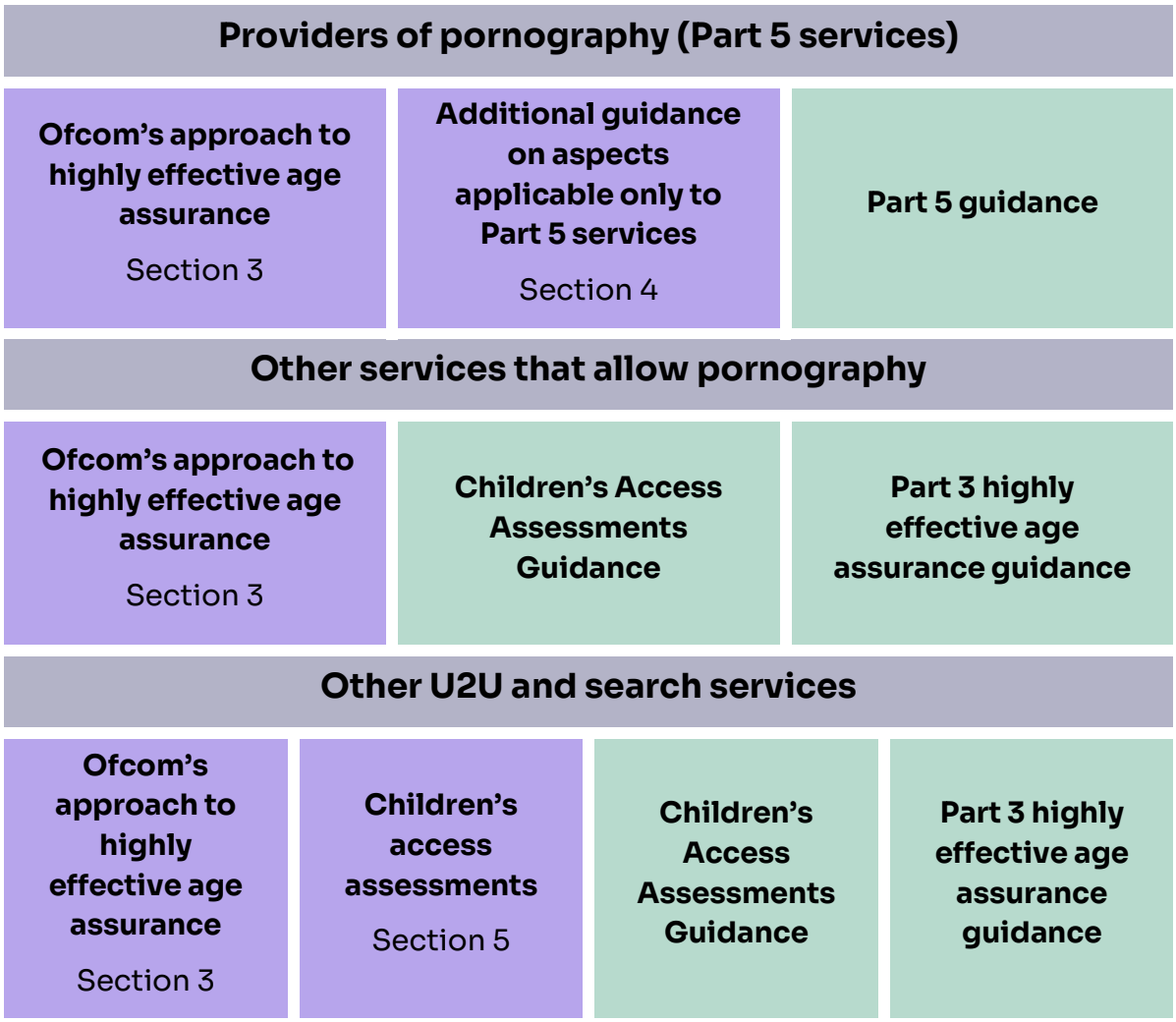
2.26 We have separately published the three pieces of guidance that we discuss in this statement:

[25] See Sections 12(4)-(6) of the Act.

- Guidance for Part 3 services on highly effective age assurance ("Part 3 HEAA Guidance")[26]
- Guidance for service providers publishing pornographic content ("Part 5 Guidance")[27]
- Children's Access Assessments Guidance [28]

2.27 Figure 2.1 below illustrates which sections of this statement (shown in purple), and which of our three guidance documents (shown in green), are likely to be relevant for different types of regulated services.

Figure 2.1 Age assurance and children's access duties and guidance



[26] Part 3 Guidance on highly effective age assurance
[27] Guidance for service providers publishing pornographic content
[28] Children's Access Assessments Guidance

Next steps

2.28 The publication of the Children's Access Assessment Guidance starts the clock for existing service providers to carry out their first children's access assessment under the Act. These must be completed by three months from the date of this statement, i.e. by **16 April 2025**.

2.29 All Part 3 services that have concluded that they are likely to be accessed by children will have three months from the publication of our final Children's Risk Assessment Guidance to carry out their first children's risk assessment. We will be publishing our Children's Risk Assessment Guidance in April 2025 to assist services in carrying out their children's risk assessments.

2.30 We will be publishing our final Protection of Children Codes in April 2025. Services in scope of the children's safety duties will need to be prepared to comply with them from July 2025, which is the date three months after the completion of their first children's risk assessment. This may include implementing highly effective age assurance for some services that allow pornography and other content harmful to children on their service.

2.31 Providers of Part 5 services are required to comply with their duties under the Act, including the requirement to use highly effective age assurance, from 17 January 2025 when the duties commence.[29]

[29] See the Online Safety Act 2023 (Commencement No. 4) Regulations 2024

3. Ofcom's approach to highly effective age assurance

In this section, we confirm our approach to highly effective age assurance.

Under the Online Safety Act 2023 ("the Act"), service providers who display or publish their own pornographic content online ("Part 5 services") are subject to a number of duties including a duty to use highly effective age assurance to ensure that children are not normally able to encounter pornographic content.

All user-to-user and search services ("Part 3 services") are required to carry out children's access assessments to determine whether they are likely to be accessed by children. As we confirm in Section 5 of this statement, service providers may conclude that they are not likely to be accessed by children if they are using highly effective age assurance with the result that children are not normally able to access the service.

Ofcom is required to produce and publish guidance for Part 5 services to assist them in complying with their duties under Part 5 of the Act. We refer to this as our "Part 5 Guidance". Section 4 of the Part 5 Guidance explains what we mean by highly effective age assurance.

We have also chosen to produce and publish guidance for regulated user-to-user and search services ("Part 3 services") to assist them in complying with their duties to implement highly effective age assurance. We refer to this as our "Part 3 HEAA Guidance". The Part 3 HEAA Guidance explains what we mean by highly effective age assurance for the purpose of the children's access assessment and wider children's safety duties. In this statement, we are not reaching any final decisions on our age assurance measures. We will finalise our age assurance measures in April and will update the Part 3 HEAA Guidance as appropriate.

Our approach to highly effective age assurance is consistent across Part 5 services and Part 3 services. To assess whether the age assurance process they are using is highly effective, service providers need to meet four criteria: technical accuracy, robustness, reliability and fairness. We are also clear that, in implementing a highly effective age assurance process, services are also bound by data protection laws, and we refer to the relevant requirements that services should adhere to.

In this section, we set out our consideration of stakeholder responses that we received on our draft Part 5 Guidance and Part 3 HEAA Guidance in respect of highly effective age assurance, together with our reasons for reaching our decisions. In Section 4 of this statement we set out our final position on the additional duties on Part 5 services.

Introduction

3.1 In this section, we cover our decisions on Ofcom's approach to highly effective age assurance. Services that display or publish their own pornographic content (i.e. Part 5 services) need to implement highly effective age assurance to ensure that "children are not

normally able to encounter" such content. U2U and search services in scope of the Act (i.e. Part 3 services) may also need to consider the concept of highly effective age assurance when carrying out children's access assessments or as part of the range of measures that they may need to implement to protect children. The concept of highly effective age assurance is consistent for Part 3 and Part 5 services, as reflected in the Part 5 Guidance and the Part 3 HEAA Guidance.

3.2 As already mentioned in the previous section, Part 5 of the Act imposes specific duties on service providers that display or publish their own pornographic content on their online services. Those duties include a duty to implement age assurance to ensure that children are not normally able to encounter such content. The age assurance must be of such a kind and used in a way that it is highly effective at correctly determining whether or not a user is a child.[30] Part 5 service providers should refer to this section of the statement to understand the stakeholder feedback we received and our subsequent decisions in relation to our interpretation of the concept of highly effective age assurance. The next section deals with the feedback received in relation to the wider requirements for Part 5 service providers.

3.3 Under the Act, all providers of Part 3 services are required to carry out children's access assessments to determine whether they are likely to be accessed by children. When carrying out children's access assessments, service providers may only conclude that it is not possible for children to access the service or part of it if age assurance is used with the result that children are not normally able to access the service or that part of it.[31] The Act does not specify the type of age assurance a service provider should use in this context. Ofcom has discretion on the approach that we deem to be most appropriate. As discussed in Section 5, we have decided that providers should only conclude that it is not possible for children to access the service where they are using highly effective age assurance. Part 3 services that wish to understand if they have highly effective age assurance in place for the purposes of children's access assessments should review this section of the statement to understand the comments we received and our subsequent decisions on the Part 3 HEAA Guidance.

3.4 Providers of services likely to be accessed by children are required to take and implement safety measures to mitigate the risks to children on the service. In particular, providers of U2U services likely to be accessed by children are required to use highly effective age assurance to prevent children from encountering primary priority content ("PPC") (pornographic content, and content promoting, encouraging or providing instructions for suicide, self-harm or eating disorders).[32] In our May 2024 consultation Protecting children from harms online ("May 2024 Consultation"), we proposed a number of measures in our draft Protection of Children Codes that we recommended for service providers to comply with the children's safety duties under the Act, including measures relating to the use of highly effective age assurance in the Protection of Children Code for user-to-user services.[33] We also published the draft Part 3 HEAA Guidance[34] to provide further detail on what was

[30] Section 81(3) of the Act.
[31] Section 35(2) of the Act.
[32] Sections 12(4), (5) and 12(6) of the Act.
[33] See Section 15 of our May 2024 Consultation.
[34] See Annex 10 of our May 2024 Consultation.

meant by the concept of highly effective age assurance, which was consistent with the draft Part 5 Guidance we published alongside our December 2023 Part 5 Consultation.

3.5 To ensure consistency in our approach, we have addressed age assurance-related responses to both our May 2024 Consultation and our December 2023 consultation, Guidance for service providers publishing pornographic content ("December 2023 Part 5 Consultation") in this section. We also set out our decisions in relation to highly effective age assurance. These are reflected in Sections 4-6 of the Part 5 Guidance, as well as the Part 3 HEAA Guidance.

3.6 As explained in Section 2, we are not making decisions on the measures we will include in our Protection of Children Codes in this document. We will set out our final decisions on the Protection of Children Codes, including the age assurance measures we consulted on, when we publish our Protection of Children statement in April 2025. We therefore do not set out our response to stakeholder comments on those measures here. We have retained references in the Part 3 HEAA Guidance to the draft Protection of Children Codes in order to ensure clarity for services as they conduct their first children's access assessments. Service providers should bear in mind that this version of the guidance is based on draft codes wording and we may update it in April 2025 when we publish our Protection of Children Statement. Beyond April 2025, we may update the guidance where necessary to reflect any future age assurance measures.

3.7 As well as in response to stakeholder comments, we have made a number of drafting and structural changes to improve the clarity and structure of the guidance, and to ensure consistency between the Part 5 Guidance and the Part 3 HEAA Guidance as appropriate. This includes some changes to the Part 3 HEAA Guidance to more closely align its structure and content with Section 4 of the Part 5 Guidance. This is because we consider it to be important that service providers in scope of Part 5 and/or Part 3 have a clear and consistent understanding of how to implement highly effective age assurance to prevent children from encountering harmful content. We have also made changes to the introduction of the Part 3 HEAA Guidance to make it clearer for services when the Part 3 HEAA Guidance is relevant to them and how it relates to the Protection of Children Codes. We have not included further reference to such changes in this section, as they do not represent changes to our policy position since consultation, and they are essentially clarificatory in nature.

Age assurance methods

Our proposals

3.8 At consultation, we proposed a non-exhaustive list of examples of the kinds of age assurance methods that we considered could be highly effective. These examples included open banking, photo-identification (photo-ID) matching, facial age estimation, mobile network operator (MNO) age checks, credit card checks, and digital identity wallets (referred to as reusable Digital ID services in our May 2024 Consultation).

3.9 We stated that age assurance methods are developing at pace and that the list may expand in time.

3.10 We said that the list was non-exhaustive and there may be other existing or emerging methods that service providers could choose to implement. In either case, we said that service providers should ensure that any such other method needed to meet our proposed

four criteria – technical accuracy, robustness, reliability and fairness – for Ofcom to consider it capable of being highly effective.

3.11 We also set out several approaches that we would not consider to be highly effective age assurance. This included self-declaration of age, age verification through online payment methods which do not require a user to be over the age of 18, and general contractual restrictions on the use of the regulated service by children.

3.12 In the draft Part 5 Guidance, we proposed a flexible approach as to who should carry out the age assurance method (i.e. whether done in-house or provided by a third-party vendor), so long as service providers to whom the Part 5 duties apply, can demonstrate that their chosen approach is highly effective at ensuring that children are not normally able to encounter pornographic content on their regulated services.

3.13 In the draft Part 3 HEAA Guidance, we went further to explain that we recognise that as well as building an in-house age assurance method, or purchasing a method from an age assurance provider, there may be wider system-level age assurance processes that service providers can use to distinguish between children and adults on their service. Regardless of who conducts the age checks, we stressed in the draft guidance that it was the responsibility of the provider of the regulated U2U service to ensure that appropriate arrangements are in place to ensure they are meeting their obligations to protect children.

3.14 We did not prescribe that an age assurance process must comprise of multiple methods, used in combination with each other, in order to be highly effective. We said at paragraph 4.9 of our December 2023 Part 5 Consultation that it is for each service provider to determine which kind(s) of age assurance are most appropriate to meet its duties under the Act. In recognition that there are likely a number of ways to implement an age assurance process that is highly effective, and that our guidance is applicable to a diverse range of services, our approach to the guidance afforded service providers a degree of flexibility in how they comply.

Summary of responses

3.15 We received a range of responses to both our December 2023 Part 5 Consultation and our May 2024 Consultation about Ofcom's approach to providing examples of kinds of age assurance that are, or are not, highly effective at correctly determining whether or not a particular user is a child.

3.16 Several respondents expressed their view that some methods included on the list at consultation are not capable of being highly effective. Some respondents suggested additional methods that were not referenced in either consultation but which they believed should be included on the list of methods that are capable of being highly effective. Some respondents argued that age assurance should be carried out at the device-based, Operating System (OS), or app store level, rather than by individual service providers.

3.17 Some respondents also queried whether multiple methods are required in order for an age assurance process to be highly effective.

3.18 We set out these comments in more detail below.

Stakeholder feedback relating to Ofcom's overall approach

3.19 The Association of Police and Crime Commissioners stated its view that Ofcom's approach allows providers flexibility to select the age assurance method that is best for their service and adapt this over time to reflect changing technology and context.[35]

3.20 Yoti argued that 'examples of age assurance methods that could be highly effective' should be phrased more explicitly as 'methods that can be effective' or 'methods that are highly effective'.[36]

3.21 Veridas argued that Ofcom should aim to be technologically neutral in its approach to the guidance and suggested that providers should be able to choose from a wider range of solutions, as long as they comply with minimum requirements.[37]

3.22 Online Dating and Discovery Association and techUK suggested that our guidance should align with the ICO and state explicitly that we do not expect services to "implement age assurance methods that: are not currently technically feasible; pose a significant and disproportionate economic impact on businesses; or pose risks to the rights and freedoms of people that are disproportionate to the other processing activities on the service."[38]

3.23 An individual respondent commented that "there is little doubt that the technical capacity to carry out age checks in a privacy-respecting and extremely reliable way already exists."[39].

3.24 The Age Verification Providers Association and Verifymy suggested that Ofcom should align the list of methods with those referenced in the ICO's Opinion on age assurance.[40]

3.25 iProov stated that Ofcom's commitment to review available age assurance methods that are capable of being highly effective in future is too vague to have an effect, because there is no formal requirement on Ofcom to do so and no timeline is presented which would bind Ofcom.[41]

Methods that we proposed are capable of being highly effective

3.26 Some respondents expressed broad support for the kinds of age assurance we suggested are capable of being highly effective,[42] while other respondents expressed concern that the age assurance technologies are still too nascent or that features of certain methods mean they are not capable of being highly effective.[43]

---

[35] Association of Police and Crime Commissioners response to our May 2024 Consultation, p.4.
[36] Yoti response to our May 2024 Consultation, p.7.
[37] Veridas response to our December 2023 Part 5 Consultation, p.2.
[38] Online Dating and Discovery Association response to our May 2024 Consultation, p.3; techUK response to our May 2024 Consultation, p.4.
[39] J. Carr response to our May 2024 Consultation, p.2.
[40] Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.3; Verifymy response to our December 2023 Part 5 Consultation p.2.
[41] iProov response to our December 2023 Part 5 Consultation, p.9.
[42] Arcom response to our December 2023 Part 5 Consultation, p.4; Barnardo's response to our December 2023 Part 5 Consultation, p.5; Match Group response to May 2024 Consultation, p.3; Te Mana Whakaatu Classification Office response to our December 2023 Part 5 Consultation, p.2.
[43] Hutchison, A. response to our December 2023 Part 5 Consultation, pp.2-3; Jackson, EM. response to our December 2023 Part 5 Consultation, pp.2-3; Name Withheld 8 response to our December 2023 Part 5

3.27 We received stakeholder feedback about the use of facial age estimation, including that the margin of error associated with such technologies makes it easier for children to circumvent them.[44] The Canadian Centre for Child Protection stated its view that too much trust has been put into facial age estimation.[45] [✂][46]

3.28 Veridas, in contrast, argued that biometric solutions "guarantee superior levels of security and protection for minors."[47] Yoti argued that its facial age estimation is recognised for its resilience against spoofing and that checks which rely on date of birth pose other challenges, are costly, and may be exclusionary.[48] TikTok suggested that age estimation models "should in principle be highly effective, if sufficiently reliable and accurate, for use on the vast majority of services."[49]

3.29 Yoti questioned the inclusion of MNO and credit card age checks. It requested that Ofcom supply the evidence obtained to suggest that these methods could be highly effective and argued that these methods cannot meet our proposed four criteria without additional authentication.[50]

3.30 The Department for Science, Innovation and Technology (DSIT) suggested that 'Digital Identity Services' is a more appropriate title than 'Digital Identity Wallets'. They explained that 'Wallets' are the technology that stores the identity attribute, whereas the attribute is what is used to check someone's age.[51] ACT - The App Association suggested that digital identities or credentials offer a high level of age assurance, and they can minimise personal data sharing, offering users more control over their identity.[52]

3.31 Yoti stated that for document-based age assurance methods to be considered highly effective they need to be mandated at a minimum that stipulates liveness detection, document authenticity checks and face matching.[53]

Consultation, pp.2-3; Fringe Dweller Productions response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 1 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 2 response to our December 2023 Part 5 Consultation, pp.2-3; Name Withheld 3 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 4 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 5 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 6 response to our December 2023 Part 5 Consultation, pp.1-3; Safazadeh, S. response to our December 2023 Part 5 Consultation, pp.1-3; Shaw, A. response to our December 2023 Part 5 Consultation, pp.1-3; Warren A. response to our December 2023 Part 5 Consultation, pp.2-4; Burville, M. response to our December 2023 Part 5 Consultation, pp.1-3; Collier D. response to our December 2023 Part 5 Consultation, pp.1-3; 14 further confidential individual respondents to our December 2023 Part 5 Consultation, pp.1-4.

[44] [✂]

[45] Canadian Centre for Child Protection response to our May 2024 Consultation, p.2.

[46] [✂]

[47] Veridas response to our May 2024 Consultation on Protecting Children from Harms Online, p.2.

[48] Yoti response to our May 2024 Consultation, p.20.

[49] TikTok response to the May 2024 Consultation, p.7.

[50] Yoti response to our December 2023 Part 5 consultation, pp.7-8.

[51] DSIT provided this suggestion during regular engagement.

[52] ACT - The App Association response to the May 2024 Consultation, p.4.

[53] Yoti response to our November 2023 Illegal Harms Consultation, p.30.

Additional methods that stakeholders suggested are capable of being highly effective

3.32 Respondents suggested additional methods to be included as capable of being highly effective.

Email-based age estimation

3.33 "Email-based age estimation" refers to a method that estimates the age of a user by analysing other online services where that user's email address has been used.

3.34 Verifymy pointed to their white paper[54] where they explain that email-based age estimation is designed to provide robust age assurance that is frictionless, privacy-preserving, inclusive and operates without discernible bias.[55]

3.35 Verifymy explained that "to successfully pass an age estimation check using an email address, it must have been used for a variety of online purposes, typically related to financial institutions, utility companies, credit providers or similar".[56]

3.36 The Age Verification Providers Association and Verifymy argued that this method can fulfil the criteria and that its inclusion would align with the solutions referenced in the ICO's Opinion on age assurance.[57] [58]

Offline verification methods

3.37 The Canadian Centre for Child Protection and Common Sense Media argued for the consideration of offline verification methods, such as a physical token obtained from retailers already equipped to verify customer age (e.g. those selling alcohol or cigarettes). The Canadian Centre for Child Protection highlighted that these could be more accessible to users, whereas Common Sense Media highlighted that these could be more privacy preserving.[59]

3.38 The Canadian Centre for Child Protection explained that the process "involves adults gaining access to a login identifier and a password that would give them access to age restricted content", pointing out that the "CNIL recommends the use of physical scratch cards as a method of offline verification".[60] [61]

---

[54] https://www.verifymyage.co.uk/press/Verifymy-White-Paper-Email-age-estimation-2024.pdf
[55] Verifymy response to our December 2023 Part 5 Consultation, p.2.
[56] Verifymy White Paper on email age estimation, June 2024, p.23.
[57] ICO, 2024, Age assurance for the children's codes. [Accessed 16 December 2024].
[58] Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.3; Verifymy response to our December 2023 Part 5 Consultation, p.2.
[59] Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, pp.3-4; Common Sense Media response to our December 2023 Part 5 Consultation, p.2.
[60] Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, p.4.
[61] The Commission nationale de l'informatique et des libertés (CNIL) is the French data protection regulatory authority.

Credit reference agency checks, the electoral roll, and National Insurance numbers

3.39 Equifax and Geocomply argued that credit reference agency checks methods can fulfil the criteria while creating little friction for users.[62]

3.40 Yoti requested that Ofcom clarify whether credit reference agency checks or the electoral roll are potentially highly effective and argued that children can circumvent this method if they know the name, date of birth and address of a family member.[63] Yoti also cautioned Ofcom against considering age assurance based on National Insurance numbers as accurate, as they considered these numbers to be easily stolen or shared.[64]

Age inference models

3.41 Most of the responses about age inference were received in response to the May 2024 Consultation.

3.42 Google argued that age inference approaches should be allowed if they are sufficiently accurate.[65] Google suggested that the model should be required to operate within "a reasonable level of accuracy" rather than a specific range, to avoid disproportionate burdens.[66]

3.43 Snap argued that such approaches can be more privacy preserving and more difficult to circumvent.[67]

3.44 The International Justice Mission argued that providers should explore the technological feasibility of detecting behaviour change that could indicate a child is using an adult platform.[68]

3.45 5Rights argued that tech companies serve age-relevant targeted advertising to children as a core feature of their business model, demonstrating that they already know which users are children. It argued that if services already know where underage children are, they should be held accountable if they do not use this information to remove them.[69]

3.46 5Rights also suggested methods such as using AI models to detect suspected underage users; making it possible for users and non-users to report underage users (e.g. via a reporting button); training moderators to consider whether accounts they are reviewing may be held by underage users and create a mechanism for human review; using keyword detection (e.g. "I am in Year 6") in their automated moderation strategy.[70]

3.47 Internet Matters argued that most digital service providers, including commercial pornography platforms, continuously gather data on users' behaviour and should use it to

---

[62] Equifax response to our December 2023 Part 5 Consultation, p.2; Geocomply response to our December 2023 Part 5 Consultation, pp.1-2.
[63] Yoti response to our December 2023 Part 5 Consultation, p.9.
[64] Yoti response to our May 2024 Consultation, p.26.
[65] Google response to our May 2024 Consultation, p.25.
[66] Google response our May 2024 Consultation, p.3.
[67] Snap response to our May 2024 Consultation, p.18.
[68] International Justice mission's response to our May 2024 Consultation, p.10.
[69] 5Rights response to the May 2024 Consultation, p.14.
[70] 5Rights response to the May 2024 Consultation, p.14.

age assure users on a continuous basis and to identify children who manage to evade an age assurance process.[71]

3.48 ACT - The App Association were critical of age inference methods, suggesting that they interfere with a child's right to privacy and offer a low level of assurance if the data quality is poor or inaccurate.[72]

3.49 Meta highlighted that they currently rely on a combination of age assurance methods and other protective measures to strengthen their age assurance. This includes using age prediction models which place appropriate restrictions on users to ensure they are in product experiences suitable for their age.[73]

Verifiable parental consent

3.50 Most of the responses about verifiable parental consent were received in response to our May 2024 Consultation.

3.51 TechUK and Apple argued that verifiable parental consent, whereby a parent or guardian undergoes an age check to approve a child's access to a platform, should be added to the list of solutions that are capable of being highly effective.[74]

3.52 TechUK suggested that parental verification can be "particularly useful for services targeting younger audiences".[75]

3.53 Epic Games explained that its method involves a parent being verified as an adult from a choice of verification methods, including face scan, ID scan, and payment card.[76]

3.54 Apple argued that effective parental confirmation of a child's age avoids the need to further process that child's data, which they feel would be an unnecessary interference with the child's privacy rights.[77]

Parental controls and content filtering

3.55 We also received responses regarding parental controls and content filtering, which are tools which enable parents or carers to exercise control over the types of experiences their children are having online, including by controlling the type of content they can access.

3.56 k-ID put forward that "well-designed and easy-to-use parental tools can support access controls and improve the efficacy and transparency of content controls, recommender systems, and reporting and complaints handling".[78]

3.57 The Association for UK Interactive Entertainment (Ukie) highlighted that these tools can ensure that young users only access content that is suitable for their age group.[79] One

[71] Internet Matters response to our December 2023 Part 5 Consultation, p.9.
[72] ACT - The App Association response to our May 2024 Consultation, p.3.
[73] Meta response to our May 2024 Consultation, p.16.
[74] Apple response to our May 2024 Consultation, p.15; techUK response to our May 2024 Consultation, p.15.
[75] techUK response to our May 2024 Consultation, p.15.
[76] Epic Games response to our May 2024 Consultation, p.13.
[77] Apple response to our May 2024 Consultation, pp.15-16.
[78] k-ID response to our May 2024 Consultation, p.3.
[79] Ukie response to our May 2024 Consultation, p.26.

respondent argued that the presence of parental controls on a platform, to mitigate the risk of harm to children, should inform the standard of proportionate age assurance required.[80]

3.58 The Family Online Safety Institute (FOSI) said parental controls and user online safety tools should not be the sole solution but instead must be part of a more comprehensive approach, warning that "any regulation about parental controls must ensure that they do not overpower parents by offering full surveillance tools that would violate minors' rights to privacy and access to information".[81]

3.59 One respondent highlighted the use of parental controls as an age assurance measure in Ireland and the EU, as well as having support from the eSafety Commissioner in Australia.[82]

3.60 Some respondents advised Ofcom to focus on content filtering at the device or ISP level.[83] Many stakeholders also expressed support for using device-level parental controls as a method of age assurance.[84]

Age assurance at the app store, device, or operating system (OS) level

3.61 Many respondents highlighted the potential effectiveness of age assurance that is carried out by providers of devices, operating systems (OS) or app stores and suggested considering the role they could play in deploying age assurance.[85]

[80] [✂]
[81] Family Online Safety Institute response to our May 2024 Consultation, p.8.
[82] Mobile Games Intelligence Forum response to our May 2024 Consultation, p.2.
[83] Burville, M. response to the our December 2023 Part 5 Consultation, p.2; Collier D. response to our December 2023 Part 5 Consultation, p.2; Fringe Dweller Productions response to our December 2023 Part 5 Consultation, p.2; Hutchison, A. response to our December 2023 Part 5 Consultation, p.3; Name Withheld 1 response to our December 2023 Part 5 Consultation, p.2; Name Withheld 2 response to our December 2023 Part 5 Consultation, p.3; Name Withheld 3 response to our December 2023 Part 5 Consultation, p.2; Name Withheld 4 response to our December 2023 Part 5 Consultation, p.2; Name Withheld 5 response to our December 2023 Part 5 Consultation, p.3; Name Withheld 6 response to our December 2023 Part 5 Consultation, p.4; Name withheld 9 response to our December 2023 Part 5 Consultation, p.2; Safazadeh, S. response to our December 2023 Part 5 Consultation, p.2; Shaw, A. response to our December 2023 Part 5 Consultation, p.3; Warren A. response to our December 2023 Part 5 Consultation, p.3; xHamster response to our December 2023 Part 5 Consultation, p.5; 14 further confidential individual respondents to our December 2023 Part 5 Consultation, p.3.
[84] Arcom response to our December 2023 Part 5 Consultation, p.7; Amaran, M. response to our May 2024 Consultation, p.2; Dr Karen Middleton, University of Portsmouth and Conscious Advertising Network response to our May 2024 Consultation, p.17; Mobile Games Intelligence Forum response to our May 2024 Consultation, p.3; xHamster response to our May 2024 Consultation, p.7; xHamster response to our December 2023 Part 5 Consultation, p.4.
[85] Advertising Association response to our May 2024 Consultation, p.11; Amaran, M. response to our May 2024 Consultation, pp.5-6; Aylo response to our December 2023 Part 5 Consultation, p.1; [✂]; Internet Matters response to our December 2023 Part 5 Consultation, p.2; Meta response to our May 2024 Consultation, pp.3-4; [✂]; Online Dating and Discovery Association response to our May 2024 Consultation, pp.3-4; [✂]; X response to our May 2024 Consultation, p.2; [✂]; [✂]; [✂].

3.62 The benefits of these approaches were cited by respondents as minimising concerns around user privacy and/or data collection,[86] eliminating the need for repetitive verification,[87] being a global and/or existing approach,[88] being cost-efficient and providing a better user experience,[89] as well as not being reliant on individual service providers complying with the legislation.[90]

3.63 Match Group suggested that app stores within the distribution layer of the online ecosystem should contribute to preventing minors from accessing adult-only content and platforms, in addition to any age assurance measures and/or default settings for child users that are employed by individual services.[91]

3.64 Integrity Institute flagged that device-level age assurance could be vulnerable to malware, viruses, and children creating apps to circumvent the age assurance system locally.[92]

3.65 Snap called for Ofcom to accelerate its report on the role of app stores as they considered that the report's findings may enable app stores to be brought in scope of the Act. They argued that this would be a "fully interoperable" approach to age assurance.[93]

Age tokens

3.66 Several responses mentioned that age tokens can allow online service providers to confirm whether users meet age requirements while minimising processing of personal data.[94]

3.67 ACT - The App Association noted that the effectiveness of age tokens depends on the age assurance method that the provider employs and that the technology to generate age tokens is not yet widely available.[95] Nevertheless, they recommend using third party age assurance providers, with their benefits including "offering tokenized age checking, API solutions, or background checks or to users directly by providing digital IDs".[96]

3.68 Yoti requested guidance on how frequently tokens ought to be reverified and the suitable cybersecurity standards to ensure the safety of tokens-based age assurance technologies.[97]

---

[86] Advertising Association response to our December 2023 Part 5 Consultation, p.11; [✂]; StripChat response to our December 2023 Part 5 Consultation, p.3; X response to our May 2024 Consultation, p.2; xHamster response to our December 2023 Part 5 Consultation, p.4 and our May 2024 Consultation, p.3; Meta response to our May 2024 Consultation, pp.15-16; WhatsApp response to our May 2024 Consultation, p.2.
[87] xHamster response to our December 2023 Part 5 Consultation, p.4; WhatsApp response to our May 2024 Consultation, p.2; Meta response to our May 2024 Consultation, pp.15-16.
[88] Aylo response to our December 2023 Part 5 Consultation, p.1; [✂]; X response to our May 2024 Consultation, p.2; Internet Matters response to our December 2023 Part 5 Consultation, p.3; [✂].
[89] xHamster response to our December 2023 Part 5 Consultation, p.4.
[90] StripChat response to our December 2023 Part 5 Consultation, p.2; xHamster response to our December 2023 Part 5 Consultation, p.4.
[91] Match Group response to our December 2023 Illegal Harms Consultation, pp.16-17.
[92] Integrity Institute response to our May 2024 Consultation, p.3.
[93] Snap response to our May 2024 Consultation, pp.17-18.
[94] 5Rights response to our May 2024 Consultation, p.14; Yoti response to our December 2023 Part 5 Consultation, p.15; ACT - The App Association response to our May 2024 Consultation, p.5.
[95] ACT - The App Association response to our May 2024 Consultation, p.5.
[96] ACT - The App Association response to our May 2024 Consultation, p.5.
[97] Yoti response to our December 2023 Part 5 Consultation, p.15.

Multiple methods

3.69 Some respondents argued that it may not be possible to meet the standard of highly effective age assurance without a service provider deploying a combination of age assurance methods. Integrity Institute argued that a "waterfall" approach combining multiple methods may be required.[98]

3.70 Online Dating and Discovery Association (ODDA) argued that highly effective age assurance should not be overly reliant on technical solutions alone but rather a multi-layered approach which improves accuracy.[99]

3.71 ODDA and techUK suggested that age estimation, when combined with other techniques in a layered or "waterfall" approach, can be less intrusive and more effective.[100]

3.72 Match Group suggested that our guidance narrowly focused on whether a single age assurance measure can meet all the criteria to the necessary degree, rather than leaving space for multiple methods to be used.[101]

3.73 Meta highlighted that no single age assurance measure is 100% effective. Therefore, they encouraged adopting a multi-layered approach, with investment in a suite of tools and to allow flexibility for new methods in the future.[102]

UK Digital Identity and Attributes Trust Framework

3.74 We received comments about the UK Digital Identity and Attributes Trust Framework ("the trust framework") in response to our December 2023 and May 2024 consultations. The trust framework is a set of rules and standards governing the provision of digital verification services across the UK economy. It helps organisations to check identities, share attributes and reuse information in a trusted and consistent way. Providers of digital identity or attribute services can become certified against the trust framework.

3.75 Open Identity Exchange (OIX) suggested that Ofcom should require that third-party age assurance providers are certified against the trust framework.[103] Ingenium Biometric Laboratories Limited recommended that Ofcom should consider how it uses or points to the standards, assurance and testing requirements and processes that are detailed in the trust framework to meet the requirements of the highly effective age assurance criteria.[104]

Our decisions

Decision regarding Ofcom's overall approach

3.76 We have considered stakeholder responses about the list of methods that are capable of being highly effective. We are satisfied that there is value in having a non-exhaustive list of methods that are capable of being highly effective to give services an indication of the

[98] Integrity Institute response to our May 2024 Consultation, p.2.
[99] Online Dating and Discovery Association response to May 2024 Consultation, p.3.
[100] Online Dating and Discovery Association response to May 2024 Consultation, p.6; techUK response to the May 2024 Consultation, p.14.
[101] Match Group response to the May 2024 Consultation, p.3.
[102] Meta response to our May 2024 Consultation, p.14.
[103] Open Identity Exchange response to our December 2023 Part 5 Consultation, p.4.
[104] Ingenium Biometric Laboratories Limited response to our May 2024 Consultation, p.8.

technology that they could use to comply with their duties. By emphasising the non-exhaustive nature of the list, we also ensure that the guidance is flexible as technology continues to develop at pace.

3.77 In addition, we are clear throughout the accompanying guidance that the outcomes of the implementation of an age assurance method by a service provider will depend on *how* the method is implemented, rather than simply which age assurance method they choose. Providers must make sure that whatever age assurance method they implement, the chosen method is highly effective at correctly determining whether or not a particular user is a child and, in making that choice, we expect them to have regard to our criteria for highly effective age assurance that we set out in both the Part 5 Guidance and Part 3 HEAA Guidance.

3.78 With regards to Yoti's comment about the framing of the list of methods, we have rephrased 'kinds of age assurance that could be highly effective' to 'kinds of age assurance that are capable of being highly effective', to better reflect our position that no form of age assurance is inherently highly effective; rather, effectiveness depends on how age assurance is implemented by the provider.

3.79 In addition, the statutory age assurance report that Ofcom is required to produce (see paragraph 3.356 below) will provide an opportunity for a stocktake on the state of the technology used by service providers.

Methods that we proposed in our consultation as capable of being highly effective

3.80 We acknowledge the circumvention risks related to credit card and MNO checks identified by Yoti in their response. We have decided, therefore, to further clarify that if a service provider wishes to implement credit card or MNO based age assurance, they should ensure a suitable level of authentication is in place. We provide further detail on this in the section on robustness in paragraphs 3.182.

3.81 With regard to Yoti's request for Ofcom's evidence to suggest that MNO and credit card checks could be highly effective, we have considered the evidence in the Arcom 2024 reference framework for age verification on pornographic sites and concluded, in line with the French regulator, that credit card checks have the potential of being a highly effective method of age verification.[105] We have taken a similar approach to MNO age checks. We recognise that this is an expanding space, with entry of new providers.[106]

3.82 In response to stakeholder feedback about the margin of error where facial age technology is used, we will consider and address the subject of minimum age and age groups in our Protection of Children Statement in April. We address concerns about the margin of error and circumvention risk associated with facial age estimation as a highly effective method of age assurance to determine if a user is over or under 18 years of age from paragraphs 3.113 on technical accuracy and 3.138 on robustness.

3.83 In response to comments on the effectiveness of photo-ID matching, we advise at paragraph 4.55 of the Part 5 Guidance and paragraph 4.32 of the Part 3 HEAA Guidance that liveness

[105] Arcom, 2024, Referential technique sur la verification [accessed 9 January 2025]
[106] VeriMe, available at https://verime.net [accessed 9 January 2025]

detection can provide further confidence that a child user has not uploaded a photo of an adult by ensuring that the user undergoing the age assurance process is present at the time the check is carried out. To address the concern that a robust photo-ID check could be easily circumvented, we have directed service providers to government issued guidance on how to detect certain fake documents at paragraph 4.57 of the Part 5 Guidance. Therefore, we remain of the view that this method is capable of being highly effective if implemented in line with the Part 5 Guidance.

3.84 In line with DSIT's suggestion, we have amended the terminology in the Part 5 Guidance at paragraph 4.18 to 'Digital Identity Services' and edited our description of these services accordingly to increase clarity for service providers.[107]

Additional methods that stakeholders suggested are capable of being highly effective

Email-based age estimation

3.85 Email-based age estimation estimates the age of a user by analysing the purposes for which the user's provided email address has been used. This could include where the email address has been used with financial institutions, utility providers and other relevant services.

3.86 Based on the evidence provided by the Age Verification Providers Association and Verifymy, we consider that this method is capable of achieving high levels of technical accuracy. There are ways to increase the robustness, for example by requiring users to verify their ownership of the email address. Where the underlying data points are based on strong digital identity verification (e.g. through banks, mortgage lenders), this is likely to indicate reliability. Finally, we consider that this method can be operated without risk of material bias, indicating fairness. We have concluded that, overall, email-based age estimation, if deployed in line with the criteria, is capable of being highly effective at determining whether or not a user is a child.

3.87 Accordingly, we have added email-based age estimation to the non-exhaustive list of age assurance methods that are capable of being highly effective (see paragraph 4.17 of the Part 5 Guidance and after paragraph 3.12 of the Part 3 HEAA Guidance).

Credit reference agency checks, the electoral roll, National Insurance numbers, and offline verification methods

3.88 We have not updated the list to include credit reference agencies, the electoral roll per Equifax and Geocomply's suggestions, or offline verification as argued for by the Canadian Centre for Child Protection and Common Sense Media. Our assessment is that, unless combined with other kinds of highly effective age assurance, these methods could all be easier for children to circumvent, because they do not typically include means of checking that the details supplied belong to the user attempting to access the service. This does not

[107] We received DSIT's response to our December 2023 Part 5 Consultation in time to assess it and update our approach to labelling Reusable Digital ID services in time for the publication of the draft Part 3 HEAA Guidance. Therefore, no change is needed to the Part 3 HEAA Guidance. We have since decided to stop using 'reusable' because digital identity services can also be used as a one-off.

mean that these methods cannot be used in combination with other methods, as part of a wider process that could be highly effective at determining whether or not a user is a child.

Age inference models

3.89 We are aware that age inference models, which analyse a user's activity while on a service to infer their age, are being increasingly tested and deployed.

3.90 We do not believe that service providers in scope of Part 5 could reasonably implement age inference methods to comply with their duty to ensure that children are not normally able to encounter pornographic content, because age assurance should be implemented either at the point of entry to the site or no pornographic content should be visible to users on entering the site before they have completed the age check.[108] An age inference model, which analyses a user's activity while on the service and over a period of time, is therefore unlikely to be highly effective in the context of Part 5.[109] We have not therefore updated the list to include age inference models, as a number of stakeholders suggested.

3.91 The same reasoning applies to service providers in scope of the proposed service-wide age assurance access control measures (measures AA1 and AA2) of the draft Protection of Children Codes, published as part of our May 2024 Consultation.[110] These measures are designed to prevent children from accessing services that are dedicated to harmful content and recommend implementing highly effective age assurance and effective access controls in a way, and at a point in the sign-in process, to prevent users from accessing the entire service unless they have been determined to be adults.

3.92 We recognise that age inference models could, in theory, play a role for service providers in scope of other draft age assurance measures (measures AA3-AA6), where children are allowed to access a service, but must be protected from harmful content that may be present on the service.[111] We will address responses made about age inference in this context when we publish the Protection of Children Statement in April 2025 and will update our Part 3 HEAA Guidance as necessary.

Verifiable parental consent

3.93 While methods for obtaining verifiable parental consent vary, they typically involve a child self-declaring their age, and their parent being prompted to undergo an age check themselves; and verify that their child has provided the correct age. While having verifiable parental consent could be proof that a user is a child, if implemented correctly, it is not the case that the absence of verifiable parental consent could be used as evidence that the user is an adult.

---

[108] 4.7 of the Part 5 Guidance.

[109] In theory there may be cases where a provider of a Part 5 service offers regulated provider pornographic content on one part of the service and other kinds of content on other parts of the service, such that it could use age inference modelling based on users' activity on those other parts of the service. However, in practice we expect such cases to be rare, if any.

[110] See May 2024 Consultation, Section 15 and draft Protection of Children Code of Practice for user-to-user services

[111] See May 2024 Consultation, Section 15 and draft Protection of Children Code of Practice for user-to-user services

3.94 For this reason, verifiable parental consent is not a relevant or appropriate method for services in scope of Part 5 to meet their duty to implement highly effective age assurance. This is because Part 5 services should use age assurance methods in a way, that results in children not normally being able to access pornographic content on their services. This reasoning also applies to service providers in scope of the draft age assurance measures in our Protection of Children Code for user-to-user services, which we will consider in our April Protection of Children Statement.

3.95 We recognise that verifiable parental consent could, in theory, play a role in supporting more age-appropriate experiences online for children, and may help services establish if a child meets the minimum age requirements in a service's terms of service.[112] We will further consider the role of verifiable parental consent in our Protection of Children Statement in April, and will update our Part 3 HEAA Guidance if necessary.

Parental controls and content filtering

3.96 Parental controls and content filtering are optional tools that enable parents and carers to exercise control over the types of experiences their children have online. Different services offer different types of parental control and content filtering tools, with a variety of functionalities, including in some cases being able to control the type of content that children can access. Parental controls are typically available for children under the age of 13 and most social media and communication services allow children aged 13+ to open an account without parental supervision.

3.97 Parental controls and content filtering offer parents and carers the ability to exercise a degree of choice over the online experiences of their children and can play an important role in supporting more age-appropriate online experiences for children, as a number of stakeholders pointed out. However, these tools are not a way for service providers to comply with their duties in relation to highly effective age assurance. While being under parental supervision could be considered evidence that a user is a child, the lack of parental supervision should never be considered as evidence that a user is over 18. Similarly, the lack of content filtering in place could not be presumed to indicate that those accessing the service are adults.

Age assurance at the app store, device, or operating system (OS) level

3.98 We have carefully considered stakeholder arguments for alternative owners of and approaches to age assurance responsibilities. The Act makes clear that the responsibility for preventing children from accessing pornographic content falls firmly on the part of the service provider where Part 5 applies. Similarly, the Act makes clear that it is the responsibility of providers of services in scope of the Part 3 duties to prevent children from encountering PPC, and to protect children in age groups judged to be at risk of harm from encountering other harmful content.

3.99 Our proposals are neutral as to who develops or makes available the highly effective age assurance solutions. Service providers may choose to use age assurance solutions offered by third parties, either integrated with their platform or that are carried out before their users

[112] See May 2024 Consultation, Section 15 and draft Protection of Children Code of Practice for user-to-user services

are able to access the relevant content or functionality, provided they can demonstrate that this approach complies with their Part 5 or Part 3 duties. In response to stakeholder feedback, we recognise that this may include implementation of age assurance by providers of app stores, operating systems, browsers or devices.

3.100 We have updated the Part 5 Guidance at paragraph 4.11 to align with the Part 3 HEAA Guidance at paragraph 4.5 and included additional detail clarifying this. This updated guidance emphasises that system-level age assurance methods may be used but that, where any such methods are used, the regulated service provider must ensure that the overall process delivers the required outcome of the duties to implement highly effective age assurance.

3.101 As part of the ongoing implementation of the Online Safety regime, Ofcom is required under the Act to produce a report by January 2027 about the use of app stores by children.[113] In particular, the report must:

- assess what role app stores play in children encountering content that is harmful to children, search content that is harmful to children or regulated provider pornographic content by means of regulated apps [114] which the app stores make available;
- assess the extent to which age assurance is currently used by providers of app stores, and how effective it is; and
- explore whether children's online safety would be better protected by the greater use of age assurance or particular kinds of age assurance by such providers, or by other measures.

3.102 In response to Snap's suggestion that Ofcom should accelerate the publication of the app store report, we do not consider that this would be beneficial for the quality of the report's findings. Sufficient time is required to allow Ofcom to gather evidence and assess properly the impact of the current duties, before determining whether children's online safety would be better protected by the greater use of age assurance by app stores.

Age tokens

3.103 Age tokens are reusable digital assets that act as a digital proxy or representation of a completed age check. They can be shared by a user across multiple services over a defined period of time as evidence that an age check has been completed. We therefore consider that age tokens are not an age assurance method per se, but could form part of a highly effective age assurance process, so long as service providers can evidence that the age check underpinning the token and the process to share this information is highly effective.

3.104 We have updated the Part 5 Guidance at paragraph 4.11 and the Part 3 HEAA Guidance at paragraph 3.6 to include reference to age tokens. Where service providers choose to use age tokens, it remains their responsibility to ensure that the initial age check and the process to share this information with the regulated service was highly effective (e.g. that it had regard to the four criteria).

[113] Section 161 of the Act.

[114] This means an app for a regulated service for use on any kind of device. Section 161(5) of the Act.

3.105 In response to Yoti's request for guidance on the frequency with which age tokens should be reverified, we reiterate that, in line with paragraph 4.59 of the Part 5 Guidance and paragraph 3.6 of the Part 3 HEAA Guidance, it is the responsibility of the service provider to assess how frequently their age assurance process, whether enabled by age tokens or otherwise, should be repeated in order to ensure that it is highly effective.

Multiple methods

3.106 It is for each service provider to determine the method, or combination of methods, that are most appropriate to meet its duties under the Act. Some providers may choose an approach that consists of multiple methods used in combination with each other to complement each other and increase the overall effectiveness. However, we have not stated that this is the only means of ensuring that an approach is highly effective, as some stakeholders suggested.

3.107 We have taken a technology-neutral, flexible approach to highly effective age assurance to afford service providers a degree of flexibility in how they comply, recognising that both pieces of guidance apply to a broad range of service providers with diverse features and design.

UK Digital Identity and Attributes Trust Framework

3.108 We have expanded the reference to the UK Digital Identity and Attributes Trust Framework in the Part 5 Guidance at paragraph 4.27 and the Part 3 HEAA Guidance at paragraph 4.7. We consider that using a method certified against the trust framework can help to support compliance with the age assurance duties. It is not mandatory for regulated services to use a provider that is certified against the trust framework, nor is it an automatic means of compliance with the age assurance duties. However, we consider that doing so could be a useful indicator of compliance, so long as the service provider can demonstrate that their approach is highly effective and has been implemented in line with Ofcom's guidance. A register of certified services is published on GOV.UK, helping individuals and businesses to choose trustworthy services.

Criteria for determining whether age assurance is highly effective

Background

3.109 Our view is that it is both the method(s) used and the way that it is implemented that determines whether an age assurance process is highly effective. For this reason, we proposed in both the Part 5 Guidance and Part 3 HEAA Guidance four criteria that service providers should have regard to when implementing age assurance, that relate to the technical performance of the age assurance process. Those four criteria are:

- **Technical accuracy:** the degree to which an age assurance method can correctly determine the age of a user under test lab conditions.
- **Robustness:** the degree to which an age assurance method can correctly determine the age of a user in unexpected or real-world conditions.
- **Reliability:** the degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.

- **Fairness:** the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.

3.110 We proposed in our December 2023 and May 2024 consultations that service providers should ensure that their age assurance process fulfils each of the criteria in order to be considered highly effective.

3.111 We recognised that there may be trade-offs in how well an age assurance method performs against each of the criteria, and service providers should determine which trade-offs are appropriate to ensure that the overall process is highly effective at correctly determining whether a user is a child.

3.112 We received a range of stakeholder responses on the proposed criteria for determining whether age assurance is highly effective, which we address in each topic below.

The technical accuracy criterion

Our proposal

3.113 In the draft Part 5 Guidance and Part 3 HEAA Guidance, we explained that the criterion of technical accuracy referred specifically to how an age assurance method can correctly determine the age of a user under test lab conditions. We used the term 'technical accuracy' to distinguish this criterion from more holistic concepts of accuracy, which may consider a broad range of factors.

3.114 In the draft Part 5 Guidance, we proposed that a service provider should carry out the following practical steps to fulfil the criterion of technical accuracy:

- ensure the method has been evaluated against appropriate metrics and record these in the written record; and
- consider implementing a 'challenge age' approach when using an estimation method.

3.115 In the draft Part 3 HEAA Guidance, we expanded on the technical accuracy criterion, stating it is fulfilled if:

- the provider has ensured that the measures which are part of the age assurance process have been evaluated against appropriate metrics to assess the extent to which they can correctly determine the age or age range of a person under test lab conditions;
- where the age assurance process used on the service involves the use of age estimation, the provider uses a challenge age approach; and
- the provider periodically reviews whether the technical accuracy of the age assurance process for the service could be improved by making use of new technology and, where appropriate, makes change to the age assurance process.

3.116 In both pieces of guidance, we included examples of metrics that we indicated could be appropriate for assessing the technical accuracy of an age assurance solution. We suggested that for age assurance methods producing binary results this could be the True Positive Rate

(TPR), False Positive Rate (FPR), and False Negative Rate (FNR).[115] We suggested that for age assurance methods that produce continuous results this could include the Standard Deviation, Mean Absolute Percentage Error (MAPE), and Cumulative Score (CS).[116]

3.117 We explained that these metrics could be derived from the service providers' own internal testing (if feasible), from testing that third-party age assurance providers have done, or from testing by an independent third party.

3.118 In both pieces of draft guidance, we explained that where age estimation methods are not technically accurate enough to correctly determine whether a user is a child within a specific age range, using a 'challenge age' can help to improve the overall effectiveness of the age assurance process by preventing or minimising borderline cases where the age estimation method incorrectly assesses a user as being an adult when they are a child.[117] In the draft Part 5 Guidance we stated that "service providers could consider implementing a 'challenge age' approach for estimation methods which are not sufficiently technically accurate within a specific age range". We went further in the draft Protection of Children Code for user-to-user services and the draft Part 3 HEAA Guidance, specifically recommending that "a challenge age should be used where a service uses age estimation".

Summary of responses

Challenge age approach

3.119 In response to our December 2023 Part 5 Consultation, the Canadian Centre for Child Protection argued that Ofcom should consider mandating a 'challenge age' as otherwise providers are unlikely to implement this procedure.[118]

3.120 Common Sense Media noted that where age estimation solutions are currently in place, they are typically used with a second kind of verification as part of a 'challenge age' approach, to account for margin of error.[119]

3.121 The Children's Commissioner for England was supportive of service providers implementing a challenge age approach and argued that it should be set at age 25 or 30 to allow an appropriate margin of error.[120]

3.122 Yoti stated that for items restricted to those aged 18 and over, such as alcohol or knives, regulators could consider higher age thresholds, such as 23 (with a 5-year buffer) or 25 (with

[115] We define what is meant by True Positive Rate (TPR), False Positive Rate (FPR), and False Negative Rate (FNR) in our Glossary in A4 and in the technical glossary in in Annex 1 of the Part 5 Guidance
[116] We define each of the metrics set out in the glossary in Annex 4 of this statement and in the technical glossary in Annex 1 of the Part 5 Guidance.
[117] The Age Check Certification Scheme's (ACCS) standards describe the 'challenge age' as "the age at which a provider of age-restricted goods, content or services may cease to require a potential customer to prove their age by means of producing evidence of their age." ACCS, 2020, Technical Requirements for Age Estimation Technologies, p.11.
[118] Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, p.2.
[119] Common Sense Media response to our December 2023 Part 5 Consultation, p.2.
[120] Children's Commissioner for England response to our December 2023 Part 5 Consultation, p.19.

a 7-year buffer), to further restrict access among 15-17 year olds to less than 0.5% or 0.2%, respectively.[121]

3.123 iProov stated that the concept of Challenge 25 is problematic. Firstly, the introduction of a second check increases the number of potential system vulnerabilities available to a malicious actor to exploit. Second, those solutions (online or physical) which rely on a human examiner are inherently vulnerable. They asserted and cited that there is ample and increasing research to show the difficulties that even expert examiners have in correctly and consistently identifying a fake image or document.[122]

3.124 One respondent argued that the 'challenge age' approach would require additional age assurance methods (overlapping with one another) such as a massive and widespread deployment of ID verification which they view as more intrusive, less privacy preserving, more costly, and not 100% effective. [123] Twelve-App stated that it is difficult to set the right age for a challenge age given that margins of error depend on certain characteristics such as gender or skin tone, but also technical conditions of the age estimation (e.g. photo quality), and referenced the Yoti White Paper[124] as evidence.[125]

3.125 One respondent argued that evidence suggests that methods with a high false rejection rate can increase the likelihood a user will try to spoof or bypass age assurance [✂]. Some users may use VPN solutions to reach services outside the scope of the Online Safety Act. They gave the example of a Challenge 33 model creating a significant inconvenience for adults up to 33 years old who are being denied legitimate access to services without additional checks and potentially delay.[126]

Additional comments about technical accuracy

3.126 Common Sense Media stated that Ofcom should make clear its expectations that services should stay abreast of technological developments within available age assurance solutions and implement them in a timely manner.[127]

3.127 Ingenium Biometric Laboratories Limited suggested that technical accuracy ought to be broken down into more detail across photo-ID matching, facial age estimation, and reusable digital identity services.[128]

3.128 xHamster raised concerns about determining “appropriate metrics” for assessing technical accuracy.[129]

---

[121] Yoti response to our May 2024 Consultation, p.21.
[122] iProov response to our December 2023 Part 5 Consultation, pp.6-9; iProov response to our May 2024 Consultation, pp.10-13.
[123] [✂]
[124] Yoti, 2023, Yoti Facial Age Estimation White Paper [accessed 9 January 2025]
[125] Twelve App response to our May 2024 Consultation, p.3.
[126] [✂]
[127] Common Sense Media response to our December 2023 Part 5 Consultation, p.3.
[128] Ingenium Biometric Laboratories Limited response to our May 2024 Consultation, p.8.
[129] xHamster response to our December 2023 Part 5 Consultation, p.5.

Our decision

3.129 For the reasons explained in our consultation, we have decided to adopt the criterion of technical accuracy as part of our Part 5 Guidance and Part 3 HEAA Guidance.

3.130 We have updated the Part 5 Guidance (paragraph 4.33) and the Part 3 HEAA Guidance (table 4.1) to state that service providers should "ensure the age assurance method(s) has been evaluated against appropriate metrics and the results indicate that the method(s) is able to correctly determine whether or not a particular user is a child under test lab conditions". We have also updated the accompanying example of non-compliance in the Part 5 Guidance accordingly. We have made these changes to make it more explicit that there should be a positive outcome from such testing, as opposed to the testing in and of itself demonstrating that a service provider has had regard to the technical accuracy criterion.

On challenge age approach

3.131 In addition to consultation responses from Canadian Centre for Child Protection, Common Sense Media, the Children's Commissioner for England and other stakeholders, we have reviewed NIST's Face Analysis Technology Evaluation report,[130] which supports our position that, to be highly effective, an appropriate challenge age should be in place for a process that relies on age estimation. All age estimation methods carry a margin of error and a challenge age approach minimises the likelihood of children being erroneously classified as adults.

3.132 We have therefore aligned the Part 5 Guidance with the draft Protection of Children Code for user-to-user services and Part 3 HEAA Guidance, to recommend that providers should implement a challenge age when they are using an age estimation method. This is to ensure consistency between the Part 5 Guidance and Part 3 HEAA Guidance, and in recognition that the use of a challenge age can help to improve the overall effectiveness of the age assurance process.

3.133 We have not, however, recommended setting a specific age for challenge age (e.g., Challenge 25 scheme for buying alcohol[131]), as this will depend on the age estimation solution in question and the overall age assurance process in place. As stated in paragraph 4.41 of the Part 5 Guidance and paragraph 4.19 of the Part 3 HEAA Guidance, the challenge age should be set according to the limits of the technical accuracy of that method. For example, where a solution is less technically accurate, a higher challenge age should be set.

3.134 In response to stakeholder comments at paragraph 3.124 of this statement that a challenge age approach may be privacy intrusive, we refer to the ICO's Opinion on Age Assurance that says, when used correctly, waterfall techniques have the potential to offer high levels of confidence, while providing a privacy respecting approach for users.[132]

Additional comments about technical accuracy

3.135 In recognition of Common Sense Media's comment about the importance of staying abreast of technological developments and implementing them in a timely manner, and to align with

[130] NIST, 2024, Face Analysis Technology Evaluation: Age Estimation and Verification
[131] Drink Aware, Challenge 25.
[132] Section 3.4, para 2 of the ICO's Opinion on Age Assurance.

the steps set out in the draft Part 3 HEAA Guidance, we have amended the Part 5 Guidance at Figure 4.2 and paragraph 4.43 to state more explicitly that providers should periodically review whether the technical accuracy of the age assurance process for the service could be improved by making use of new technology and, where appropriate, make changes to the age assurance process.

3.136 We acknowledge the suggestion at paragraph 3.127 that technical accuracy could be broken down into further detail for specific age assurance methods. However, we consider that the metrics we have suggested in both pieces of guidance are suitable for use across a range of methods which produce binary or continuous outputs. We have therefore made no changes to the technical accuracy criterion based on this suggestion; however, we will remain actively engaged in how the testing of different methods develops in time.

3.137 We acknowledge the concern expressed by one respondent about determining appropriate metrics to assess the technical accuracy of an age assurance method; however, we consider that the metrics we have suggested in both pieces of guidance, for both binary and continuous methods, help to mitigate this concern.

The robustness criterion

Our proposals

3.138 In the draft Part 5 Guidance and draft Part 3 HEAA Guidance, we stated that the criterion of robustness **describes** the degree to which an age assurance method can correctly determine the age of a user in atypical or real-world conditions.

3.139 We explained that conditions in the real world will vary considerably to those in a test scenario, and that common threats to robustness in the context of age assurance methods include:

- conditions that change the quality or characteristics of an input e.g. poor lighting, blurring, brightness, contrast, or positioning of the user in an image (relevant for methods reliant on visual input e.g., facial age estimation, photo-ID matching, etc.); and
- circumvention techniques that are easily accessible to children and where it is reasonable to assume they may use them (for example a child user uploading an image of an ID that does not belong to them).

3.140 We recognised that, if an age assurance method is not robust, it will be more vulnerable to circumvention. We also acknowledged that no age assurance method is likely to be effective all the time and in all circumstances.

3.141 In the draft Part 5 Guidance, we proposed that a service provider should carry out the following practical steps to fulfil the criterion of robustness:

- implement age assurance processes that have undergone tests in multiple environments during development, and include details of this test process in the written record; and
- take steps to mitigate against methods of circumvention that are easily accessible to children and where it is reasonable to assume that children may use them.

3.142 In line with our duty under Part 5 of the Act to provide examples of circumstances in which we are likely to consider that a provider has not complied with its duties, we outlined the following examples:

- the service provider has implemented facial age estimation which allows children to upload a still image they have obtained of an adult;
- the service provider has implemented photo-ID matching which easily allows children to verify their age using fake or manipulated ID documents;
- the service provider explicitly and deliberately encourages or enables child users to circumvent its age assurance process and/or access controls, e.g., by providing a link to and recommending the use of a VPN to avoid the controls, such that they are not likely to be effective at normally preventing children from encountering regulated provider pornographic content.

3.143 In the draft Part 3 HEAA Guidance, we proposed that the robustness criterion is fulfilled if the service provider has:

- taken steps to identify methods children use to circumvent the age assurance process used on the service to determine that the relevant individual is not a child;
- taken feasible and proportionate steps to prevent children using those methods; and
- ensured that the age assurance process for the service have been tested in multiple different environments during the development of the age assurance process.

Summary of responses

3.144 Several respondents expressed support for the proposals outlined above.[133] Other respondents highlighted additional circumvention risks, suggested further mitigations, or ways that the evidence and understanding of circumvention risks could be increased. We explain these comments in more detail below.

Threats to the robustness of age assurance methods

Facial age estimation

3.145 iProov expressed concern about the circumvention risks associated with facial age estimation arguing that the evidence on the lack of accuracy of such technologies, as illustrated by NIST in testing, makes it easier for children to circumvent them than is the case when using age verification technologies.[134]

3.146 The Canadian Centre for Child Protection argued that facial age estimation using only a static image is not sufficiently reliable, given the circumvention risks.[135]

3.147 [✂][136]

3.148 On the other hand, Yoti argued that its facial age estimation solution is recognised for its resilience against spoofing.[137]

---

[133] Brown, N. response to our December 2023 Part 5 Consultation, p.3; Northern Ireland Commissioner for Children & Young People (NICCY) response to the May 2024 Consultation, p.31; Nexus response to the May 2024 Consultation, p.14.
[134] iProov response to our December 2023 Part 5 Consultation, p.1.
[135] Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, p.4.
[136] [✂]
[137] Yoti response to our May 2024 Consultation, p.20.

Methods reliant on passports or other ID documents

3.149 iProov stated that age verification based on a user uploading hard identifiers, such as a passport, could be circumvented by a child making use of an adult's documents.[138]

3.150 Yoti argued that sophisticated fake identity documents can be purchased at a very low price and should be considered accessible to children.[139] Geocomply provided an example of this occurring.[140]

3.151 Several respondents noted the use of AI tools to create more sophisticated false documents or enable circumvention in other novel ways[141] and 5Rights highlighted this as an important emerging risk which service providers should monitor.[142]

Credit card checks

3.152 Common Sense Media and ID Crypt Global expressed concern that a child could circumvent credit card verification as a form of age assurance by using a parent's credit card.[143]

3.153 ID Crypt Global argued that providing a credit or debit card does not confirm the identity of the person holding the card but instead confirms the identity of the card owner.[144]

3.154 Common Sense Media stated that since the enactment of Children's Online Privacy Protection Rule (COPPA) in the United States in 1998, credit card verification has become the "most circumvented method of age assurance".[145]

Open banking

3.155 With regards to methods that check age via a user's bank account, one respondent argued that a child could make use of an adult's details to circumvent the solution, showing how this method proposed by Ofcom may be circumvented.[146]

3.156 Open Identity Exchange suggested that when using a bank account login as proof of identification, users should have to use a biometric authenticator to prove they are the owner of the bank account, otherwise it is easy for someone to borrow the bank account of an adult for ID proofing purposes.[147]

---

[138] iProov response to our December 2023 Part 5 Consultation, p.3.
[139] Yoti response to our December 2023 Part 5 Consultation, p.11.
[140] Geocomply response to our December 2023 Part 5 Consultation, p.3.
[141] 5Rights response to our December 2023 Part 5 Consultation, p.8; Christian Action Research and Education (CARE) response to our December 2023 Part 5 Consultation, p.4; GeoComply Solutions response to our December 2023 Part 5 Consultation, p.3; Qoria Ltd response to May 2024 Consultation, p.3.
[142] 5Rights response to our December 2023 Part 5 Consultation, p.8.
[143] Common Sense Media response to our December 2023 Part 5 Consultation, pp.3-4; ID Crypt Global response to our December 2023 Part 5 Consultation, p.2.
[144] ID Crypt Global response to our December 2023 Part 5 Consultation, p.2.
[145] Common Sense Media response to response to our December 2023 Part 5 Consultation, p.4.
[146] [✂]
[147] Open Identity Exchange (OIX) response to our December 2023 Part 5 Consultation, p.2.

Virtual Private Networks (VPNs)

3.157 A large number of respondents cited VPNs as a threat to the robustness of age assurance methods.[148] Some respondents felt that the use of VPNs will render the approach to highly effective age assurance ineffective overall and that it is not possible to mitigate against the circumvention risk that they pose.[149]

3.158 Many respondents suggested that Ofcom could mandate that service providers block traffic from VPNs.[150] Internet Matters called for Ofcom to strengthen its stance on VPNs, setting a higher bar for service providers to mitigate against people using VPNs to circumvent age assurance.[151] Dr Karen Middleton, University of Portsmouth and Conscious Advertising Network argued that this could be achieved by service providers using algorithms to detect and block known VPN IP addresses, blocking proxy servers, requiring two-factor authentication, using parental controls and blacklisting VPNs. This respondent also called on

---

[148] Barnardo's response to our December 2023 Part 5 Consultation p.6; Burville, M response to our December 2023 Part 5 Consultation, pp.3-4; CEASE's response to our December 2023 Part 5 Consultation p.4; Christian Institute's response to our December 2023 Part 5 Consultation pp.3-4 and our May 2024 Consultation, p.10; Collier D, response to our December 2023 Part 5 Consultation, pp.3-4; CARE's response to our December 2023 Part 5 Consultation p.4; Dr Karen Middleton, University of Portsmouth and Conscious Advertising Network response to our May 2024 Consultation, p 16; Common Sense Media's response to our December 2023 Part 5 Consultation P.4; Fringe Dweller Productions response to our December 2023 Part 5 Consultation, pp.3-4; Hutchison, A response to our December 2023 Part 5 Consultation, p.5; Inkbunny response to our May 2024 Consultation, p.3; Internet Matters response to our December 2023 Part 5 Consultation, p.10; Jackson, EM response to our December 2023 Part 5 Consultation, p.4; Name Withheld 1 response to our December 2023 Part 5 Consultation, pp.3-4; Name Withheld 2 response to our December 2023 Part 5 Consultation, pp.3-4; Name Withheld 3 response to our December 2023 Part 5 Consultation, pp.3-4; Name Withheld 4 response to our December 2023 Part 5 Consultation, pp.3-4; Name Withheld 5 response to our December 2023 Part 5 Consultation, pp.3-4; Name Withheld 6 response to our December 2023 Part 5 Consultation, pp.5-6; Name Withheld 8 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 9 response to our December 2023 Part 5 Consultation, p.3; Safazadeh, S, response to our December 2023 Part 5 Consultation, pp.3-4; Shaw, A. response to our December 2023 Part 5 Consultation, pp.3-4; Warren techUK response to our May 2024 Consultation, p.15; Yoti response to our May 2024 Consultation, pp.5-6 and November 2023 Illegal Harms Consultation, p.7; 14 further confidential individual respondents to our December 2023 Part 5 Consultation, pp.3-4.

[149]Burville, M response to our December 2023 Part 5 Consultation, p.5; Collier D, response to our December 2023 Part 5 Consultation, pp.4-5; Fringe Dweller Productions response to our December 2023 Part 5 Consultation, p.4; Hutchison, A response to our December 2023 Part 5 Consultation, p.5; Jackson, EM response to our December 2023 Part 5 Consultation, p 4; Name Withheld 1 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 2 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 3 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 4 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 5 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 6 response to our December 2023 Part 5 Consultation, p.6; Name Withheld 8 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 9 response to Part 5 guidance, p.3; Safazadeh, S, response to our December 2023 Part 5 Consultation, p.4; Shaw, A. response to our December 2023 Part 5 Consultation, p.4; Warren A, response to our December 2023 Part 5 Consultation, p.4; 14 further confidential individual respondents to our December 2023 Part 5 Consultation, pp.1-4.

[150] Barnardo's response to our December 2023 Part 5 Consultation p.6; CARE's response to our December 2023 Ofcom's Part 5 consultation p.4; CEASE's response to our December 2023 Part 5 Consultation p.4; Christian Institute's response to our December 2023 Part 5 Consultation, p.4. and our May 2024 Consultation, p.10; Dr Karen Middleton, University of Portsmouth and Conscious Advertising Network response to our May 2024 Consultation, p.16.

[151] Internet Matters response to our December 2023 Part 5 Consultation, p.10.

Ofcom to work with legislators to implement further legislation to require VPN providers to comply with the act.[152]

3.159 Christian Action Research and Education (CARE) and the Centre to End All Sexual Exploitation (CEASE) suggested that providers should require age assurance each time a user tries to access content through a VPN including access from a known VPN IP address, even if this is based outside the UK. [153]

3.160 On the other hand, a group of individual respondents highlighted that VPNs are used by adults for many reasons, including by adult content creators who are vulnerable to hackers trying to find out their locations.[154]

3.161 Yoti highlighted that video sharing platforms and on-demand programme services block VPNs, and encouraged Ofcom to look at the approach that they take.[155]

The dark web, proxy websites or servers, and Tor Browsers

3.162 Common Sense Media also noted that there are a range of other technologies that enable children to access age-restricted content, including torrenting media content,[156] using proxy websites or servers, using a Tor Browser, and accessing the 'dark web.' It cited a BBFC survey showing that as many as 25% of children aged 14-15 and 33% of children aged 16-17 reported knowing how to use these tools to circumvent age assurance.[157] It argued that these services are often hard to identify, are decentralised, and designed to evade law enforcement, making them difficult to mitigate against.[158]

Device and account sharing

3.163 Some respondents commented on the circumvention risk of device and/or account sharing.[159]

---

[152] Dr Karen Middleton, University of Portsmouth and Conscious Advertising Network response to our May 2024 Consultation, pp.16-17.
[153] CARE's response to our December 2023 Part 5 Consultation p.4; CEASE's response to our December 2023 Part 5 Consultation p.5.
[154] Burville, M response to our December 2023 Part 5 Consultation, p.4; Collier D, response to our December 2023 Part 5 Consultation, p 4; Fringe Dweller Productions response to our December 2023 Part 5 Consultation, p.4; Hutchison, A response to our December 2023 Part 5 Consultation, p 5; Jackson, EM response to our December 2023 Part 5 Consultation, p 6; Name Withheld 1 response to our December 2023 Part 5 Consultation, p 4; Name Withheld 2 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 3 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 4 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 5 response to our December 2023 Part 5 Consultation, p.4; Name Withheld 6 response to our December 2023 Part 5 Consultation, p.6; Name Withheld 8 response to our December 2023 Part 5 Consultation, p 4; Safazadeh, S, response to our December 2023 Part 5 Consultation, p.4; Shaw, A. response to our December 2023 Part 5 Consultation, p.4; Warren A, response to our December 2023 Part 5 Consultation, p.5; 14 further confidential individual respondents to our December 2023 Part 5 Consultation, p.4.
[155] Yoti response to our May 2024 Consultation, pp.5-6.
[156] A peer-to-peer file sharing protocol.
[157] BBFC, 2020, Young people, Pornography & Age-verification [accessed 9 January 2025]
[158] Common Sense Media's response to our December Part 5 Consultation, p.4.
[159] Bandio's response to our May 2024 Consultation, pp.3-4; International Justice Mission response to our May 2024 Consultation, p.7; Roblox response to our May 2024 Consultation, p.21.

3.164 Yoti cautioned against one-off age checks because of the problems this may pose with device or account sharing.[160]

3.165 Open Identity Exchange expressed concern about the use of stored ID proofs from reusable IDs and argued that without an appropriate authentication mechanism, a reusable ID could be easily shared among users.[161]

Stakeholder views on mitigations to circumvention risks

3.166 Some respondents suggested repeating age checks as a way of mitigating circumvention risks.[162] The Age Verification Providers Association suggested that a user's age should be checked every 1-3 months.[163] Yoti highlighted that the recent consultation from French regulator, Arcom, considered that providers hosting pornography should require an age check every time a user attempts to access their service.[164] Veridas argued that there is a need for a successive authentication process, even when passwords are used, as passwords can be stolen or guessed.[165] The National Crime Agency (NCA) highlighted that it may be useful to consider requiring periodic ongoing age assurance for a user to continue to access a service, such as after a set period of time or a change to the risk of a user's profile. This may help to mitigate against any users incorrectly passing an age check.[166]

3.167 The Age Verification Providers Association suggested that rather than Ofcom seeking to define countermeasures for any given method of age assurance, it should require that methods meet the minimum requirement for highly effective age assurance and monitor to ensure that service providers put surveillance in place to ensure their services are not normally encountered via circumvention methods.[167]

3.168 Yoti suggested that liveness checks should be mandatory for any facial age estimation solution.[168]

3.169 The Age Check Certification Scheme suggested that service providers should be required to bind the result of an age assurance check to a user.[169]

3.170 Common Sense Media and Integrity Institute argued that requiring a combination of age assurance checks, otherwise called a "waterfall" approach, is an effective means of reducing the risk of circumvention.[170] Arcom highlighted that the more user-friendly an age assurance

[160] Yoti response to our May 2024 Consultation, p.27.
[161] Open Identity Exchange's response to our December 2023 Part 5 Consultation p.3.
[162] Age Verification Providers Association response to our December 2023 Part 5 Consultation, pp.7-8; Internet Matter's response to our December 2023 Part 5 Consultation, p.6; Veridas response to our December 2023 Part 5 Consultation, p.4; Yoti response to our May 2024 Consultation, p.27.
[163] Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.7.
[164] Yoti's response to our May 2024 Consultation, p.27.
[165] Veridas response to our December 2023 Part 5 Consultation, p.4.
[166] National Crime Agency (NCA) response to our May 2024 Consultation, p.9.
[167] Age Verification Providers Association response to our December 2023 Part 5 Consultation, pp.8-9.
[168] Yoti's response to our December 2023 Part 5 Consultation, p.12.
[169] Age Check Certification Scheme response to our May 2024 Consultation, p.41.
[170] Common Sense Media response to our December 2023 Part 5 consultation, p.4; Integrity Institute response to our May 2024 Consultation, p.2.

process is, the less likely it is to be circumvented, so service providers should deploy user-friendly solutions.[171]

Additional comments about circumvention and robustness

3.171 Yoti argued that Ofcom's proposals did not account for the ease of circumvention, the evolution of circumvention techniques (for example virtual private networks), and users' literacy levels. It argued that these are important factors for service providers to consider when implementing an age assurance method and that they should form the basis of an additional criteria.[172]

3.172 The Free Speech Coalition expressed concern that service providers would not be able to determine the circumvention risk of technologies. They suggested that our guidance should define acceptable risk and how to calculate this.[173] Similarly, xHamster called for further clarification on how service providers should assess which circumvention methods might be considered as easily accessed by children.[174]

3.173 One respondent argued that the risk of circumvention is inevitable unless a service provider implements "extremely intrusive and technically unfeasible verification and continuous monitoring methods". The respondent said this indicates why it is essential to approach child safety online through a number of ways, including education of the general public and strengthening parental controls, rather than placing the burden solely on the service provider.[175]

3.174 Some respondents suggested that Ofcom should do more to build the evidence base and awareness of circumvention techniques. Several respondents suggested that Ofcom should conduct research on circumvention techniques.[176] Nexus suggested that Ofcom should continually scope for software that might be able to bypass age assurance technology.[177] Yoti suggested that Ofcom should in the future provide examples, or anonymised examples, of sites that demonstrate best practice to protect their users.[178]

Our decision

3.175 For the reasons explained in our consultation, we have decided to adopt the criterion of robustness as part of our Part 5 Guidance and Part 3 HEAA Guidance. Having carefully considered the consultation responses on this criterion, we discuss below what changes we have, and have not made, in relation to what we say in the Part 5 Guidance and the Part 3 HEAA Guidance on this criterion.

---

[171] Arcom response to our December 2023 Part 5 Consultation, p.5.
[172] Yoti response to our December 2023 Part 5 Consultation, p.12.
[173] Free Speech Coalition response to our December 2023 Part 5 Consultation, p.5.
[174] xHamster response to our December 2023 Part 5 Consultation, p.6.
[175] [✂]
[176] Children's Commissioner for England response to Part 5 Consultation, p.17; REPHRAIN response to our May 2024 Consultation, p.3; Yoti's response to our December 2023 Part 5 Consultation, p.13; Yoti's response to Ofcom's our May 2024 Consultation, pp.27-28.
[177] NEXUS response to our May 2024 Consultation, p.14.
[178] Yoti response to our May 2024 Consultation, p.27.

Changes to our guidance concerning robustness

3.176 In response to stakeholder feedback, we have strengthened our guidance on mitigating circumvention risks in a number of ways below.

Robustness criterion

3.177 We have refined the definition of the robustness criterion in the Part 5 Guidance and the Part 3 HEAA Guidance to state that it "describes the degree to which an age assurance method can correctly determine the age of a user in actual deployment contexts", rather than "in unexpected or real-world conditions", as stated previously. We have reflected this throughout both pieces of guidance.

3.178 In the Part 5 Guidance at paragraph 4.52 and the Part 3 HEAA Guidance at paragraph 4.29, we have refined one of the steps under the robustness criterion to state that service providers should "identify and take appropriate steps to mitigate against methods of circumvention that are easily accessible to children and where it is reasonable to assume that children may use them" to align both pieces of guidance and to provide further clarification.

3.179 For consistency and clarity, we have made clear in the Part 3 HEAA Guidance at paragraph 4.37 and the Part 5 Guidance at paragraph 4.60, that the robustness criterion means that "service providers should not publish content on their service that directs or encourages UK users to circumvent the age assurance process or the access controls, for example by providing information about or links to a virtual private network (VPN) which may be used by children to circumvent the age assurance process". This alignment change has been made to ensure that both pieces of Guidance are consistent on this point, and because we think it is important to make it clear it is a facet of robustness.

Facial age estimation

3.180 We have considered stakeholder feedback regarding circumvention risks associated with facial age estimation. Concerns that the margin of error associated with facial age estimation technologies could enable circumvention are addressed through the use of the challenge age approach, which is outlined under the technical accuracy criterion (at paragraph 3.131).

3.181 In response to Yoti's comment, we have amended both pieces of guidance to state more explicitly that liveness detection should help to ensure that children are not using still images of adults to pass through facial age estimation or photo-ID matching (see paragraphs 4.55 and 4.56 of Part 5 Guidance and 4.33 of Part 3 HEAA Guidance).

Methods reliant on ID documents, mobile phone number, email address, or credit card checks

3.182 In response to stakeholder concerns around circumvention, we have stated in our final guidance that, where service providers implement an age assurance process that relies on details obtained via a user's identification document (including digitally stored proofs), mobile phone number, email address, or credit card details, we expect providers to have a means of checking that the details supplied belong to the user attempting to access the service (see paragraph 4.53 of the Part 5 Guidance and paragraph 4.30 of the Part 3 HEAA Guidance). We have added a corresponding example of non-compliance to the Part 5 Guidance at paragraph 4.60.

Frequency of age checks

3.183 Based on stakeholder responses, we have stated in our final guidance that repeating an age check can help to increase the robustness of an age assurance method, and that services providers should: i) consider whether repeated age checks may be needed to secure the robustness of their solution based on the features of their service and age assurance process; and ii) determine how often it is appropriate to repeat an age check (see paragraph 4.58 of the Part 5 Guidance and paragraph 4.36 of the Part 3 HEAA Guidance).

3.184 We consider that this change helps to address a range of circumvention-related stakeholder concerns, including device or account sharing and instances where children may be mistakenly classified as adults during the initial age check (although where a service provider has had sufficient regard to the criteria, such instances should be rare).

3.185 We have also suggested that, when deciding on the frequency of age checks, services should be mindful of data protection law requirements to assess the necessity and proportionality of the personal data processing and to take a data protection by design approach to implementing the data protection principles. We have also signposted services to the relevant ICO Guidance.

3.186 However, we have not made any further recommendations about the frequency of any repeat age checks. This is because the need for repeat age checks, and the appropriate approach to conducting these, is likely to vary depending on the context of each service and its age assurance process. Given that we allow flexibility over the age assurance process used, service providers themselves should consider the potential use of repeat age checks in their specific circumstances.

Areas where we do not consider changes to our guidance are necessary

Access to falsified documents

3.187 We acknowledge Yoti's concern about children's potential access to sophisticated falsified documents. We have made a minor clarification in the Part 5 Guidance at paragraph 4.57 and the Part 3 HEAA Guidance at paragraph 4.34 to remove the qualifier 'basic' and state that we expect service providers to take steps to detect falsified documents, such as those set out in government-issued guidance on how to prove and verify someone's identity ("GPG45"). Where a service provider has made no effort to ensure that an age assurance process reliant on hard identifiers is able to detect falsified documents, we would likely consider that the provider has not taken sufficient steps to ensure that the approach is robust. We also make clear in the 'example of non-compliance' (see paragraph 4.60 of the Part 5 Guidance) that, if a service provider has implemented photo-ID matching which easily allows children to verify their age using fake or manipulated ID documents, we are likely to consider that they have not complied with their duties.

3.188 We have considered stakeholder concerns about generative artificial intelligence ("Generative AI") enabling greater access to sophisticated forged identity documents.[179] Both the Part 5 Guidance and the Part 3 HEAA Guidance make clear that we expect service

[179] Generative AI refers to artificial intelligence models that can create text, images, audio and videos in response to a user prompt.

providers to take appropriate steps to mitigate against methods of circumvention that are easily accessible to children, and where it is reasonable to assume that children may use them. Therefore, should such methods become easily accessible and widely used by children, the current wording in both pieces of guidance makes clear that we will expect providers to take appropriate action to mitigate these risks.

VPNs, the dark web, proxy websites or servers, and Tor Browsers

3.189 We have carefully considered stakeholder responses that suggested that we should require providers to block VPNs or other technologies that could be used by children to access age-restricted content, such as proxy websites or servers and Tor Browsers.

3.190 The Part 3 and Part 5 duties in the Act do not require services to block all traffic from VPNs or other similar private network technologies – which are lawful to use in the UK. This means that Ofcom has no power to mandate this. Additionally, there are no duties in the Act which require providers of such VPN or private network services to age assure their own users. It would be a matter for Parliament to decide whether any such duties should be imposed on providers of regulated services or providers of VPN or private network services.

3.191 We have set out in both the Part 5 Guidance and the Part 3 HEAA Guidance that service providers should ensure that they take appropriate steps to mitigate against methods of circumvention that are easily accessible to children or where it is reasonable to assume that they may use them. This does not mean, however, that they are required to block access via VPNs or similar technologies entirely for the above-mentioned reasons.

3.192 We have also explained in both the Part 5 Guidance at paragraph 4.60 and the Part 3 HEAA Guidance at paragraph 4.37 that service providers should not publish content on their service that directs or encourages UK users to circumvent the age assurance process or the access controls, for example by providing information about or links to a VPN. We have aligned the wording on this point in the Part 5 Guidance, so that it is the same as the wording we had used in the proposed Part 3 HEAA Guidance.

Additional comments about circumvention and robustness

3.193 We agree with Yoti's argument that ease of circumvention, the evolution of circumvention techniques, and users' literacy levels are important factors for service providers to consider when implementing age assurance. However, we do not consider it necessary to create an additional criterion in the Part 5 Guidance or Part 3 HEAA Guidance to reflect these factors, because they are incorporated in the criterion of robustness, which requires service providers to take appropriate steps to mitigate circumvention attempts, and the principle of accessibility, which suggests that age assurance should be easy to use and work for all users.

3.194 We have not made any changes to the guidance in response to requests for more detailed guidance on acceptable levels of circumvention risk and how to calculate it. While we acknowledge that no age assurance method is likely to be effective all the time and in all circumstances, we expect service providers to take appropriate steps to mitigate against methods of circumvention that are easily accessible to children, and where it is reasonable to assume that children may use them.

3.195 We do not agree that the risk of circumvention would require a service provider to implement "extremely intrusive and technically unfeasible verification and continuous monitoring methods". We consider that it is technically feasible to implement highly

effective age assurance whilst having due regard to the importance of protecting user privacy. The ICO stated its support for this approach in its response to our December 2023 Consultation and our May 2024 Consultation.[180]

3.196 We note responses that suggested that Ofcom should do more to build the evidence base and awareness of circumvention techniques. We consider that the report on the use of age assurance, to be published 18 months after the regulations come into force, will provide us with a good first opportunity to assess, as necessary and appropriate, any circumvention techniques or solutions that threaten to reduce the effectiveness of age assurance, as well as examples of industry good practice for dealing with them.

The reliability criterion

Our proposal

3.197 In the draft Part 5 Guidance and Part 3 HEAA Guidance, we stated that the criterion of reliability describes the degree to which the output from an age assurance method is reproducible and derived from trustworthy evidence.

3.198 We explained that reproducibility describes the ability for an age assurance method to perform in a consistent manner, producing the same or similar outputs when given the same or similar inputs.

3.199 We explained that strength of evidence describes the relative weight that should be afforded to the underlying data or documents used as evidence to determine a user's age. It concerns how trustworthy the documents or data are and therefore is indicative of how much reliance, or doubt, a service should place on the output of an age assurance method derived from this evidence.

3.200 In the draft Part 5 Guidance, we proposed that a service provider should carry out the following practical steps to fulfil the criterion of reliability:

- ensure that age assurance methods with a degree of variance (e.g., methods that rely on statistical modelling or artificial intelligence) have been suitably tested, and that ongoing performance is measured and monitored; and
- ensure that the evidence that the age assurance method uses is derived from a trustworthy source.

3.201 In the case of methods with a degree of variance, we provided examples of key performance indicators that service providers could consider in this regard, such as the age verification accuracy rate (AVAR) and age verification efficiency (AVE).[181]

3.202 In the draft Part 3 HEAA Guidance, we proposed that the reliability criterion is fulfilled if:

- The provider has taken steps to ensure that where age assurance methods forming part of the age assurance process rely on artificial intelligence or machine learning:

[180] ICO response to our December 2023 Part Consultation; ICO response to our May 2024 Consultation, p.4.
[181] The Age Verification Accuracy Rate (AVAR) is the percentage of users correctly identified as belonging to the appropriate age group; Age Verification Efficiency (AVE) is the time taken to complete the age verification process.

- the artificial intelligence or machine learning has been suitably tested during the development of the age assurance process to ensure it produces reproducible results;
- the artificial intelligence or machine learning is regularly tested to ensure it produces reproducible results;
- the outputs of the artificial intelligence or machine learning used are monitored and assessed against key performance indicators designed to identify whether the artificial intelligence or machine learning produces reproducible results; and
- in circumstances where the artificial intelligence or machine learning used are observed to be producing unreliable or unexpected results, the root cause of the issue is identified and rectified.

- The provider has taken steps to ensure that any data relied upon as part of the age assurance process comes from a reliable source.

3.203 In the draft Part 5 Guidance and Part 3 HEAA Guidance, we provided a non-exhaustive list of aspects of the relevant evidence that service providers might wish to consider in deciding whether the evidence is trustworthy. We provided examples of features that would indicate trustworthy evidence when using photo-ID matching, drawing from the Government's Good Practice Guide (GPG45) which provides guidance to businesses on how to prove and verify someone's identity.

Summary of responses

3.204 xHamster suggested that it would be useful for Ofcom to provide more guidance on what would constitute a reliable or trustworthy source and suitable data for testing.[182] Global Network Initiative also wanted Ofcom to clearly articulate what would be a reliable source for data.[183]

Our decision

3.205 For the reasons explained in our consultation, we have decided to adopt the criterion of reliability as part of our Part 5 Guidance and Part 3 HEAA Guidance.

3.206 For consistency and clarity across both pieces of guidance, we have:

a) updated all instances where we refer to a "reliable source" to a "trustworthy source".
b) aligned the suggested steps under the reliability criterion in the Part 5 Guidance (paragraphs 4.66 – 4.74) with those included in the Part 3 HEAA Guidance (paragraphs 4.38 – 4.50). We have also refined the steps in both pieces of guidance, to make clear our expectation that the first step refers to testing during the development of the age assurance process, and the second and third steps refer to monitoring and measuring once the age assurance process has been deployed.

3.207 In response to calls for further clarity on what would constitute a trustworthy source, we have clarified at paragraph 4.73 in the Part 5 Guidance and paragraph 4.50 in the Part 3

[182] xHamster response to our December 2023 Part 5 Consultation, p.6.
[183] Global Network Initiative response to our May 2024 Consultation, p.12.

HEAA Guidance that certification against the trust framework indicates that the evidence used by a third-party digital identity or attribute service provider should be reliable.

The fairness criterion

Our proposal

3.208 In the draft Part 5 Guidance, we set out that the criterion of fairness describes the extent to which an age assurance method avoids bias and discriminatory outcomes. In the draft Part 3 HEAA Guidance, we elaborated on this definition, stating that it describes the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.

3.209 The fairness criterion refers to the internal operation of an age assurance method, as opposed to external factors, such as a lack of access to a particular form of identification required by the age assurance method. These are additional important considerations that come under the principle of accessibility, which we provide further detail on in paragraph 4.86 of the Part 5 Guidance and paragraph 4.66 of the Part 3 HEAA Guidance.

3.210 Bias or discriminatory outcomes in the context of the fairness criterion could include, for example, where an age assurance method provides outputs with a lower degree of technical accuracy for users of certain ethnicities when relying on facial age estimation.

3.211 We stated that ensuring that the age assurance process is fair will help to ensure that it does not prevent adults from accessing legal content in a discriminatory way. We also consider that this criterion is important to assist service providers to comply with the duties under the Equality Act 2010, which prohibits discrimination against persons sharing protected characteristics. The relevant characteristics in this instance include race, age, disability, sex, and gender reassignment.

3.212 In the draft Part 5 Guidance, we proposed that to have regard to fairness a service provider should ensure that, where relevant, the age assurance method used has been tested on diverse datasets. We explained that this step applies specifically to age assurance methods which rely on machine learning or statistical modelling. This is because bias in this context may occur when the datasets used to train an algorithm are not sufficiently diverse.

3.213 In the draft Part 3 HEAA Guidance, we proposed that the fairness criterion is fulfilled if the provider has ensured that any elements of the age assurance process for a service, which rely on artificial intelligence or machine learning, have been tested and trained on data sets which reflect the diversity in the target population.

Summary of responses

3.214 The Children's Commissioner for England stated strong support for the consideration of the impact that discriminatory outcomes have on the effectiveness of the assurance method. The Commissioner encouraged Ofcom and the Government to develop guidance and a framework for the development of age assurance tools that are free from bias.[184]

[184] Children's Commissioner for England response to our May 2024 Consultation, p.5.

3.215 xHamster queried how service providers can ensure that any third-party age assurance provider they use effectively mitigates bias and discriminatory outcomes. [185]

3.216 Multiple respondents raised issues of accuracy and biases associated with age estimation,[186] such as it being less accurate for women, girls, or those from ethnic minorities,[187] with iProov making this point in relation to NIST testing.

3.217 The Integrity Institute suggested that technical accuracy is often compromised because models are rarely trained on globally representative data. It argued that age estimation models require much better training data, including a large and diverse sample of individuals below and above 18 years of age from various backgrounds to ensure an acceptable margin of error.[188]

3.218 In Yoti's response to the Illegal Harms Consultation, they highlighted the need for regulators to assess "transparency and require independent review to assess the origin of AI datasets, bias levels and accuracy of artificial intelligence approaches." Yoti also stressed the need to have an expectation of businesses doing the appropriate due diligence when choosing an age assurance supplier such as the legality of their training data capture.[189]

3.219 The Northeastern University London argued that humans are already biased estimators of age, and AI age estimation tools have been shown to further exaggerate these biases. They also highlighted concerns that reliance on methods that use ID documents or credit cards will further widen the digital divide, given that that not all adults are able to access the necessary documentation or acquire a credit card.[190]

3.220 Yoti argued that fairness is not the correct term to use for this criterion and that "equity" might be better suited. It argued that Ofcom should be more thorough in its description of fairness and draw reference to the 'Fitzpatrick scale'[191] to prevent inequality harms.[192]

3.221 The Age Verification Providers Association recommended that in the longer term, Ofcom should set a tolerance level for 'outcome error parity'[193] to make sure that it is not at a level which has an observable impact on groups of users with protected characteristics, but at this stage it would be sufficient for providers to be aware of and publish the expected outcome.[194]

---

[185] xHamster response to our December 2023 Part 5 Consultation, p.7.
[186] Canadian Centre for Child Protection response to November 2023 Illegal Harms Consultation, p.32; Integrity Institute response to our May 2024 Consultation, pp.2-3; iProov response to our May 2024 Consultation, p.3; Northeastern University London response to our May 2024 Consultation, p.2.
[187] ACT - The App Association response to our May 2024 Consultation, p.3; Match Group response to the May 2024 Consultation, p.3; iProov response to Our May 2024 Consultation, p.3.
[188] Integrity Institute response to our May 2024 Consultation, p.3.
[189] Yoti response to November 2023 Illegal Harms Consultation, p.12.
[190] The Northeastern University London response to our May 2024 Consultation, p.2.
[191] The Fitzpatrick scale is a classification system for human skin colour that estimates how a person's skin will react to sunlight.
[192] Yoti response to our November 2023 Part 5 Consultation, p.12.
[193] We define what is meant by 'outcome error parity' in the Glossary in A4.
[194] Age Verification Providers Association response to November 2023 Part 5 Consultation, p.6.

Our decision

3.222 For the reasons explained in our consultation, we have decided to adopt the fairness criterion as part of our Part 5 Guidance and Part 3 HEAA Guidance.

3.223 For consistency and clarity, we have:

a) Updated the definition of the fairness criterion in the Part 5 Guidance at paragraph 4.75 to align with the Part 3 HEAA Guidance (paragraphs 4.51 – 4.61), to state that it describes "the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes".
b) Refined one of the suggested steps under the fairness criterion in the Part 5 Guidance at paragraph 4.77 to align with the Part 3 HEAA Guidance at paragraph 4.53, to state that service providers should "ensure that any elements of the age assurance process which rely on artificial intelligence or machine learning have been tested or trained on data sets which reflect the diversity in the target population."

3.224 We acknowledge respondents' concerns about the fairness implications of facial age estimation. As stated in paragraph 3.257, the independent evidence base on the state of facial age estimation and how it performs across different demographics is currently limited. The NIST reports and age assurance providers' self-reported metrics indicate that depending on the algorithm tested, and how it is tested, there are differences in how facial age estimation technologies perform across people of different skin tones, countries of birth, and sex.[195] In response to the Integrity Institute's comment, we recognise the importance of training age estimation models on large, diverse datasets that reflect the target population to ensure that performance is consistent across different demographics.

3.225 We acknowledge stakeholder feedback on how providers can effectively mitigate bias and discriminatory outcomes and recognise the Age Verification Providers Association's suggestion that the outcome error parity of an age assurance method can be a useful indicator of fairness. Whilst there is not currently sufficient evidence to support setting a threshold for this metric, we agree that at this stage, it is nonetheless important for service providers to have regard for outcome / error parity. We have therefore expanded both the Part 5 Guidance (paragraphs 4.78 – 4.82) and the Part 3 HEAA Guidance (paragraphs 4.54 – 4.58) to include details about outcome / error parity and to suggest that for methods reliant on artificial intelligence or machine learning, service providers should ensure the age assurance method(s) has been evaluated against the outcome / error parity, and the results indicate that the method(s) do not produce significant bias or discriminatory outcomes, as part of demonstrating how they have had regard to the fairness criterion.

3.226 In response to stakeholder comments about how service providers can ensure that any third-party age assurance provider they use effectively mitigates bias and discriminatory outcomes, service providers should be satisfied that their approach fulfils the fairness criterion and include relevant details in their written record, regardless of whether they have developed the approach themselves or procured a solution from a third-party age assurance provider. This could include details about the data sets used to train the age

[195] NIST, 2024, Face Analysis Technology Evaluation: Age Estimation and Verification, pp.1-6. [accessed 9 January 2025)

assurance method and, as we now suggest in both pieces of guidance, the outcome / error parity level. Where a third-party age assurance provider does not make relevant information available about its products, it may not be possible for a service provider to evidence that using those products fulfils the relevant criteria. In our sub-section on 'Assessing and monitoring effectiveness' from paragraph 3.350 we explain how service providers are expected to assess any third-party age assurance methods they may use, including any training data. We note Yoti's comments in relation to the use of the Fitzpatrick scale. However, we have not drawn reference from the Fitzpatrick scale as we understand that its use for the purpose of quantifying racial sensitivity of algorithms is contested.[196]

3.227 We note also Northeastern University London's concerns around a widening digital divide from service providers relying on certain age assurance methods. As set out in the Part 5 Guidance at paragraph 4.90 and the Part 3 HEAA Guidance at paragraph 4.66, we expect service providers to consider what steps are most appropriate for their service to take to ensure their age assurance process is accessible, including offering a variety of age assurance methods to increase user choice and access.

3.228 In response to the feedback from the Children's Commissioner for England, we consider that the approach we have set out in the Part 5 Guidance and Part 3 HEAA Guidance on the fairness criterion makes clear that age assurance should be implemented in a way that secures it is free from bias. We therefore do not consider it necessary for Ofcom to develop further dedicated guidance and a framework for the development of age assurance tools that are free from bias at this stage.

Setting thresholds for highly effective age assurance

Our proposal

3.229 In our December 2023 Part 5 Consultation, we explained that we had not seen sufficient evidence to help us recommend specific metrics for what constitutes highly effective age assurance.[197]

3.230 Furthermore, as the age assurance industry is nascent, with improvements and new solutions likely to emerge over time, we considered it would not be appropriate to set a base level or score for each of the criteria that service providers must ensure their age assurance method or process meets. We also expressed a desire to allow space for innovation in the online safety tech sector to continue to develop and improve age assurance solutions.

3.231 Although we did not propose specific metrics that the age assurance method(s) used should achieve for each of the criteria, we welcomed evidence from relevant stakeholders relating to the effectiveness of any of the kinds of age assurance included in the guidance, or any additional kinds of age assurance not mentioned.

3.232 In Section 15 of our May 2024 Consultation, we explained that we proposed to maintain consistency in our criteria-based approach to highly effective age assurance when

[196] NIST, 2024, Face Analysis Technology Evaluation: Age Estimation and Verification, pp.26-27. [accessed 9 January 2025]

[197] See paragraph 4.12 of our December 2023 Part 5 Consultation.

developing our final guidance and Codes relating to age assurance across Part 3 and Part 5 of the Act. We explained that, in line with the approach in the draft Part 5 Guidance, we were also proposing a criteria-based approach to highly effective age assurance. In Section 4 of our May 2024 consultation, we also proposed services providers should consider whether their age assurance was highly effective for the purposes of the children's access assessment in conjunction with our draft guidance on highly effective age assurance.

Summary of responses

3.233 The ICO stated its support for the criteria and agreed that any assessment made by a provider should be informed by multiple, interrelated criteria rather than being based solely on meeting a threshold for a single accuracy measure.[198]

3.234 A selection of respondents expressed support for the four criteria but argued that Ofcom should specify a metric to measure each of them.[199] The Christian Institute said that the four criteria were a step in the right direction but felt that the appropriate standard for meeting each of those criteria was not clear.

3.235 Two civil society respondents and the Age Verification Providers Association argued that a lack of acceptable 'False Positive Rate'[200] or no outcome-based measure will lead to a "race to the bottom".[201] Common Sense Media felt that the draft Part 5 Guidance only requires services to implement the best currently available age assurance rather than evolving with technological advances.[202]

3.236 A group of individual respondents claimed that it is nearly impossible to benchmark what would be considered highly effective.[203]

3.237 The Age Check Certification Scheme disagreed with Ofcom's assessment in the December 2023 Consultation that there is not 'sufficient evidence as to the effectiveness and potential

---

[198] ICO response to our December 2023 Part 5 Consultation, p.4.

[199] Christian Institute response to our December 2023 Consultation, p.3; NSPCC response to our May 2024 Consultation, pp.44-46; Online Safety Act Network response to our December 2023 Part 5 Consultation, pp.5-6, and response to our May 2024 Consultation, pp.72-73; Verifymy response to our December 2023 Part 5 Consultation, p.4; Yoti response to our December 2023 Part 5 Consultation, p.10.

[200] We set out what is meant by 'false positive rate' in our Glossary in A4 and in the Technical Glossary in Annex 1 of the Part 5 Guidance.

[201] Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.4; CARE response to our December 2023 Part 5 Consultation, p.4; CEASE response to our December 2023 Part 5 Consultation, p.4.

[202] Common Sense Media response to our December 2023 Part 5 Consultation, p.3.

[203] Burville, M response to our December 2023 Part 5 Consultation, p.1-2; Collier D, response to our December 2023 Part 5 Consultation, p 1-2; Fringe Dweller Productions response to our December 2023 Part 5 Consultation, p.1; Hutchison, A response to our December 2023 Part 5 Consultation, p 2; Jackson, EM response to our December 2023 Part 5 Consultation, p 2; Name Withheld 1 response to our December 2023 Part 5 Consultation, p 1; Name Withheld 2 response to our December 2023 Part 5 Consultation, p.2; Name Withheld 3 response to our December 2023 Part 5 Consultation, p.1; Name Withheld 4 response to our December 2023 Part 5 Consultation, p.1; Name Withheld 5 response to our December 2023 Part 5 Consultation, p.2; Name Withheld 6 response to our December 2023 Part 5 Consultation, p.2; Name Withheld 8 response to our December 2023 Part 5 Consultation, p 2; Safazadeh, S, response to our December 2023 Part 5 Consultation, p.1; Shaw, A response to our December 2023 Part 5 Consultation, p.1-2; Warren A, response to our December 2023 Part 5 Consultation, p.2; 14 further confidential individual respondents to our December 2023 Part 5 Consultation, p.1-4

risks of different age assurance methods to recommend specific metrics for assessing whether or not any given age assurance method or process should be considered highly effective', and referred to the 2023 Measurement of Age Assurance Technologies Report as providing evidence for this.[204] [205]

3.238 Some stakeholders suggested methods or approaches to setting thresholds. Online Safety Act Network (OSAN) said that, in their view, metrics did not preclude innovation in this field, and suggested that Ofcom should specify a metric for each of the four criteria. OSAN suggested that if, in practice, the application of the age assurance method "falls beneath the metric specified, the written record could then be used by Ofcom to determine whether providers had used their best efforts…to ensure its effective implementation".[206]

3.239 Yoti argued that Mean Absolute Error (MAE) and levels of circumvention are appropriate metrics for determining whether age assurance is highly effective. For levels of circumvention, they suggested that Ofcom undertake research into what people with varying skills and resources can do to circumvent different methods.[207]

3.240 Yoti also suggested merging the four criteria into one 'precision' category and aligning to international standards to include percentages.[208] The Integrity Institute suggested that precision and recall should be used to evaluate the effectiveness of an age assurance solution and that desired levels should be established, whilst noting that no system can achieve 100% accuracy, and there will always be a trade-off between privacy, user burden, and accuracy.[209]

3.241 The Age Verification Providers Association suggested that Ofcom should set a minimum level of accuracy for the expected outcome of any method or combination of methods. They claimed that it is possible to test any given method of age assurance to assess its effectiveness, both in terms of its headline false positive rate and "to a more sophisticated degree in terms of the distribution of errors either side of the true age".[210] They suggested that, in the future, Ofcom should explore setting a threshold for 'outcome error parity',[211] in order to measure against the 'fairness' criteria.[212]

3.242 A group of respondents argued that the draft Part 5 Guidance was too focussed on the process for implementing highly effective age assurance and should instead set an expectation for the overall outcome of an age assurance process.[213] iProov criticised Ofcom

---

[204] Age Check Certification Scheme response to our December 2023 Part 5 Consultation, p.1.
[205] Age Check Certification Scheme, 2023, Measurement of Age Assurance Technologies [accessed 9 January 2025]
[206] Online Safety Act Network response to our May 2024 Consultation, pp.72-73.
[207] Yoti response to our December 2023 Consultation, p.10.
[208] Yoti response to our December 2023 Part 5 Consultation, p.12; and our May 2024 Consultation, p.16.
[209] Integrity Institute response to our May 2024 Consultation, p.13.
[210] Age Verification Providers Association response to our December 2023 Part 5 Consultation, pp.4-6
[211] We define what is meant by 'outcome error parity' in the Glossary in A4.
[212] Age Verification Providers Association response to our December 2023 Part 5 Consultation, pp.4-6.
[213] Age Verification Providers Association response to our December 2023 Part 5 Consultation, pp.5-6; Baroness Benjamin response to our December 2023 Part 5 Consultation, pp.1-2; Lord Bethell response to our December 2023 Part 5 Consultation, pp.1-2; CARE response to our December 2023 Part 5 Consultation, p.3; CEASE response to our December 2023 Part 5 Consultation, pp.2-4.

for suggesting that specified inputs are sufficient without giving quality requirements, conformity with recognised standards or independent testing. They also stated that without a clear expectation of the outcome service providers should achieve, they were unlikely to be able to implement age assurance that is highly effective. To remedy this, they recommend that Ofcom includes a requirement to comply with relevant international standards.[214]

3.243 The Age Verification Providers Association and Lord Bethell proposed an accuracy metric that should equate to the outcome or expected outcome of a highly effective age assurance process.[215] NSPCC suggested that a process should be defined as highly effective if they have a 'true positive rate' of 95% of under 18s correctly estimated.[216] [217] The Age Check Certification Scheme suggested that highly effective age assurance should meet a 'classification accuracy' rate of 99%.[218] The Age Verification Providers Association suggested that highly effective age assurance systems should demonstrate that their "certified expected outcomes" are such that more than 95% of children under 18 and more than 99% of children under 16 are prevented from accessing PPC.[219] Similarly, Baroness Benjamin suggested an outcome based approach with thresholds for 99% compliance for under 16s and 95% compliance for 16-18 year olds.[220] Barnardo's pointed to Yoti's 2023 Facial Age Estimation White Paper to argue that a 99.91% 'true positive' rate would be an appropriate outcome metric.[221] Barnardo's also suggested that the Google age estimation model has been assessed by the Age Check Certification Scheme to accurately estimate the age of a person who is 18 as being under the age of 25 with 99.9% reliability.[222]

3.244 Match Group suggested that most services will not have a sample set of underage people from all over the world that can be used to test the model against and so will find it very difficult to determine how accurate their detection is.[223]

3.245 Some respondents suggested that Ofcom's guidance should refer to technical standards. 5Rights suggested that this should be underpinned by standards currently in development e.g. International Organization for Standardization (ISO),[224] European Telecommunications Standards Institute (ETSI)[225] and Institute of Electrical and Electronic Engineers (IEEE).[226]

---

[214] iProov response to our May 2024 Consultation, p.15.
[215] Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.5; Lord Bethell response to our December 2023 Part 5 Consultation, p.3.
[216] NSPCC response to our May 2024 Consultation, p.44.
[217] We define what is meant by 'true positive rate' in our Glossary in A4 and in the technical glossary in in Annex 1 of the Part 5 Guidance.
[218] Age Check Certification Scheme response to our May 2024 Consultation, p.2.
[219] Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.5.
[220] Baroness Benjamin response to our December 2023 Part 5 Consultation, p.2.
[221] Yoti, 2023, Yoti Facial Age Estimation White Paper [accessed 9 January 2025).
[222] Age Check Certification Scheme, available at https://accscheme.com/registry/age-estimation/google-inc-llc/ [accessed 9 January 2025].
[223] Match Group response to the May 2024 Consultation, p.3.
[224] ISO, ISO/IEC CD1 27566-1 [accessed 9 January 2025).
[225] ETSI [STF 681(TCHF) Special Task Force on Age Verification.
[226] IEEE, IEEE 2089.1-2024 Standard for Online Age Verification. [accessed 9 January 2025]

They encouraged Ofcom to also draw on the work of euCONSENT and CEN-CENELEC.[227] [228] iProov suggested that Ofcom should consider recommending compliance with recognised standards such as ETSI TS 119 461, the recognised standard for identity proofing.[229] [230] They proposed that other relevant standards could include the forthcoming standard from CEN CENELEC on biometric data injection attacks (TS 18099)[231], a complement to ISO/IEC 30107-4:2024,[232] the accepted standard for detection of presentation attacks, and the work of ISO on image capture quality and biometrics (a family of modality specific standards are being developed by ISO/IEC JTC 1/SC 37).[233]

3.246 Some techUK members suggested that Ofcom should point to the incoming IEEE and ISO standards (IEEE 2089.1 and ISO/IEC 27566) which will give percentage levels as performance indicators of age assurance processes. They suggested that without these percentages, service providers may find it hard to comply with their duties. They also highlighted that the Age Check Certification Scheme registry and the NIST facial age estimation benchmark both detail the accuracy of age assurance technologies from a range of vendors.[234]

3.247 iProov also referenced the ISO,[235] ETSI and CEN standards to suggest that testing of outcomes could be undertaken against common international standards.[236]

3.248 Ingenium Biometric Laboratories Limited suggested that, in contrast to photo ID and digital identity, the international standards for age estimation that could be used as the basis for a definition of technical accuracy have not been developed fully by industry and international partners. They recommended that Ofcom engages with a broad community of partners to support their development.[237]

3.249 There were respondents that suggested our draft guidance did not meet the will of Parliament. They argued that there was an expectation that Ofcom would set a level of proof akin to 'beyond reasonable doubt'. They suggested that this demonstrates the intention for an outcomes-based approach to highly effective age assurance.[238]

3.250 One respondent welcomed that the draft Part 5 Guidance identified the dynamic nature of the age assurance technology sector and left the possibility open for emerging new

[227] CEN-CENELEC available at cwa18016_2023.pdf (cencenelec.eu). [accessed 9 January 2025]
[228] 5Rights response to our December 2023 Part 5 Consultation, pp.1-2.
[229] ETSI, ETSI TS 119 461 [accessed 9 January 2025].
[230] iProov response to our May 2024 Consultation, p. 2.
[231] EAB, Presentation of the CEN CENELEC prTS 18099: Biometric Data Injection Detection [accessed 9 January 2025].
[232] ISO, Information technology – biometric presentation attack detection [accessed 9 January 2025].
[233] ISO, ISO/IEC JTC 1/SC 37 [accessed 9 January 2025].
[234] techUK response to our May 2024 Consultation, p.3.
[235] ISO, ISO/IEC CD1 27566-1 [accessed 9 January 2025).
[236] iProov response to our May 2024 Consultation, p.15.
[237] Ingenium Biometric Laboratories Limited response to our May 2024 Consultation, p.9.
[238] Barnardo's response to our December 2023 Part 5 Consultation, p.4; Christian Institute response to our May 2024 Consultation, p.10; Lord Bethell response to our December 2023 Part 5 Consultation, pp.1-2; Baroness Benjamin response to our December 2023 Part 5 Consultation, pp.1-2.

technologies to meet the requirements without complex legislative or regulatory processes.[239]

Our decision

3.251 Having carefully considered responses that suggest Ofcom should set numerical thresholds to define or clarify the meaning of highly effective age assurance, we remain of the view that the approach we outlined at consultation will secure the best outcomes for the protection of children online in the early years of the regime. We acknowledge, however, that numerical thresholds may complement the criteria-based approach in the future, pending further developments in testing methodology, industry standards, and independent evidence on the performance and capabilities of different age assurance methods. We elaborate on this below and explain the work that Ofcom is planning to carry out to build our evidence base in this regard.

3.252 We note that, in our consultation, we conflated the concepts of numerical thresholds and performance metrics. These are separate but related concepts; for example, in theory it is possible to set a numerical threshold (such as 95% or 99%) for a performance metric (such as True Positive Rate). In the December 2023 Part 5 Consultation, we referred to our provisional decision not to specify 'metrics'. We wish to clarify that, although we did provide various examples of relevant metrics in Annex A1 and para 4.34/4.35 of the consultation, we meant that we did not intend to specify numerical thresholds for any particular metrics at this time.[240]

3.253 We have balanced the arguments for setting numerical thresholds at this stage against the following considerations:

- the benefits of encouraging service providers to consider multiple factors to ensure an approach is highly effective;
- the limited availability of independent evidence on the performance of different age assurance methods that could help to set a threshold;
- the lack of consistent, comparable testing methodologies across the methods that are capable of being highly effective;
- the lack of industry-defined performance standards for age assurance methods; and
- the impact that setting thresholds at this stage may have on innovation and growth in the market.

3.254 We considered respondents' views that, without prescribed numerical thresholds, Ofcom's proposed criteria-based approach will not be successful. The criteria-based approach recognises that, in practice, there is more to ensuring an approach is "highly effective" than achieving a numerical threshold for a particular metric or set of metrics. This is because technology performs differently when deployed as part of wider systems and processes – for example, when deployed alongside other technologies.

3.255 The technical criteria of technical accuracy, robustness, reliability, and fairness are all important, and the complexity behind them cannot easily be captured in a single numerical

[239] [✂]

[240] See paragraph 4.12 and 4.13 of our December 2023 Part 5 Consultation.

target. We believe that this complexity is best captured by the detailed requirements on services to establish how their age assurance process meets the four technical criteria, in order to meet the overall objective that children are not normally able to access pornographic content (Part 5 services) or are prevented from encountering harmful content (Part 3 services) within the relevant deployment context. We consider that this will lead to the best outcomes for the protection of children online in the early years of the regime and do not consider that it would be appropriate to introduce numerical thresholds for one or more of the criteria at this time.

3.256 We consider in the future that numerical thresholds might have a role to play as an indicator of compliance to complement the overall criteria-based approach. For example, we acknowledge that there could be value in recommending that service providers have regard to the criteria of technical accuracy, robustness, reliability and fairness, supplemented by one or more indicative benchmarks for technical accuracy. We recognise that such an approach could potentially further help ensure that the age assurance process is sufficiently accurate, while still maintaining the vital considerations of robustness, reliability, and fairness, which are inherently less amenable to quantify through a single metric and threshold.

3.257 However, we are not in a position to set this kind of numerical threshold at this stage because of a lack of robust evidence and testing methodology to support it. In particular, having analysed the available evidence, we consider that there is high variance in results drawn from independent testing methodologies and that they are highly sensitive to test design and conditions. For example, the available evidence for facial age estimation methods demonstrates that technical accuracy results are highly sensitive to a wide range of factors such as image quality and features such as sex, skin tone, and expression.[241] This means that the same age assurance method could return different accuracy results, depending on the testing conditions, including the datasets used for testing purposes.

3.258 Ofcom has worked alongside the ICO to achieve alignment and consistency between the online safety and data protection regimes where appropriate, including establishing the effectiveness of age assurance solutions. As part of this work, in 2023, we published a joint research report which explored ways of measuring the accuracy levels achievable by different age assurance solutions.[242] This report demonstrated the complexity of this work and found that further research was needed on how to measure the overall effectiveness of age assurance methods.

3.259 We expect that the age assurance market will continue to develop at pace in the next 12-18 months, with promising developments already underway. This is largely in response to new regulation, including implementation of highly effective age assurance under the Act, as well as legislation in other jurisdictions. In this rapidly evolving space, where there is not yet a consensus on consistent, robust and comparable testing, nor a sufficiently established evidence base from such testing, any numerical threshold risks not being representative of existing technical performance, nor future-proof. Setting a threshold prematurely could also

[241] NIST, 2024, Face Analysis Technology Evaluation: Age Estimation and Verification, pp.1-6; Yoti, 2023, Facial Age Estimation White Paper [accessed 9 January 2025].
[242] Age Check Certification Scheme, 2023, Measurement of Age Assurance Technologies (2023).

preclude the use of certain methods which are rapidly improving with time, but may not achieve consistent scores under testing yet, thereby dampening innovation and unduly limiting choice. Allowing the market to develop before setting a threshold will better help to ensure that the overall age assurance landscape is diverse, trusted, accessible, and highly effective, resulting in better protections for children and better experiences for adult users.

3.260 We are undertaking a range of activities, independently and with key stakeholders in the UK and internationally, to ensure our guidance on highly effective age assurance keeps pace with technological developments and continues to reflect best practice, including the potential for setting numerical thresholds in the future. Per paragraph [3.356] of this statement, our report on the use of age assurance, which we will publish in 2026, will provide us with a good first opportunity to assess the effectiveness of age assurance methods and any circumvention techniques or solutions that threaten to reduce their effectiveness.

3.261 Ofcom is carrying out a longer-term programme of work to obtain additional evidence on age assurance methods. We anticipate that this programme will help to further develop our understanding of the capabilities of current age assurance methods and how those capabilities can map on to the criteria we laid out in the Part 5 Guidance and Part 3 HEAA Guidance. We are also following closely the work of the British Standards Institute (BSI), ISO and IEEE to develop technical standards for age assurance, and note that early iterations of some standards have been published already. We are observers of the work on the ISO/IEC 27566 standard which is aimed at setting a common framework for age assurance systems, which is due to report on Part 1 of its work in 2025.[243] We remain committed to the work to drive forward the development of technical standards. As such, we will continue to monitor and assess whether these standards are sufficiently aligned to our criteria. If we consider in due course that conformance with such technical standards would help service providers to demonstrate compliance with their duties under the Act, we will update our guidance to reflect this.

Privacy, data protection and security concerns with highly effective age assurance

Our proposal

3.262 In the draft Part 5 Guidance and the draft Part 3 HEAA Guidance, we made clear that all age assurance methods involve the processing of personal data, and as such, service providers who implement them are subject to the requirements of the UK's data protection regime in addition to their duties under the Act.[244]

[243] ISO, ISO/IEC CD1 27566-1 [accessed 9 January 2025).

[244] Under section 22(3) of the Act, when deciding on, and implementing, safety measures, services have a duty to have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy. Under section 81(4)(b), services have a duty to make and keep a written record, in an easily understandable form, of the way in which the provider, when deciding on the kinds of age

3.263 We recommended that service providers should consult relevant ICO guidance when implementing age assurance to understand how to comply with the data protection regime, including its guides to the data protection principles, identifying an appropriate lawful basis, and how to respond to users exercising their individual rights afforded by the UK GDPR.[245]

3.264 We recommended that service providers consult the Commissioner's Opinion.[246] The Opinion outlines how the data protection principles and other requirements can be considered in the context of age assurance.

3.265 We provided examples of how providers can record that they have had regard to user privacy, including conducting a Data Protection Impact Assessment (DPIA), providing privacy information to users, keeping a written record of processing activities, having a record of which staff have completed any data protection training programme that is in place, and clearly documenting technical and organisational security measures.

3.266 We stated that where we have concerns that a provider has not complied with its obligations under data protection laws, we may refer the matter to the ICO.

3.267 In the draft Part 3 HEAA Guidance only, we stated that we had recommended in the draft Protection of Children Codes that service providers should familiarise themselves with the ICO's Children's code, a statutory code of practice which sets out 15 standards that internet society services likely to be accessed by children should conform with to protect children's information rights online. We stated that service providers seeking to comply with the Part 3 duties should take the standards of the Children's code into account when implementing highly effective age assurance.[247]

3.268 In the draft Part 5 Guidance, we included an illustrative case study which provides an example of how the proposed criteria and principles might apply to an age assurance process. In this case study, as well as referring to steps taken by services to comply with their duties under the Act, we included details to demonstrate how a service's compliance with UK data protection legislation might also factor into the process by highlighting the stage at which a provider would link to relevant transparency requirements.

---

verification or age estimation and how they should be used, has had regard to the importance of protecting United Kingdom users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a regulated service (including, but not limited to, any such provision or rule concerning the processing of personal data).

[245] ICO, 2023. A guide to the data protection principles; ICO, A guide to lawful basis; and ICO, Individual rights – guidance and resources. [accessed 9 January 2025].

[246] ICO, 2024, Age Assurance for the Children's Codes.[accessed 9 January 2025].

[247] A summary of the 15 standards can be found at ICO, 'Code standards' in Age appropriate design: a code of practice for online services. [accessed 20 March 2024].

Summary of responses

General stakeholder comments about user privacy and data protection

3.269 The ICO expressed support for both pieces of guidance and the recommendation that providers should familiarise themselves with data protection legislation and how to apply it to age assurance methods.[248]

3.270 In response to our December 2023 Part 5 Consultation, the ICO stated its support for the requirement for service providers to use age assurance to ensure that children are not normally able to encounter regulated provider pornographic content. The ICO also recognised that the processing of children's data by adult sites is a valid and significant concern and that preventing child access to such sites will also help to protect children from data protection harms.[249]

3.271 The ICO emphasised that implementing a type of age assurance from Ofcom's list of methods that are capable of being highly effective will not guarantee that that the processing of personal data will be compliant with data protection law, and suggested that both the Part 5 Guidance and the Part 3 HEAA Guidance could refer to Section 6 of the ICO Opinion on Age Assurance,[250] which sets out the data protection expectations for services using age assurance, including data protection by design.[251]

3.272 Many respondents expressed concern about the amount of personal data that would be collected and/or processed because of providers implementing age assurance.[252] Big Brother Watch and the Integrity Institute warned about the risk of data breaches or leaks

[248] ICO response to our November 2023 Part 5 Consultation, pp.2-3; ICO response to our May 2024 Consultation, pp.5-7.
[249] ICO response to our November 2023 Part 5 Consultation, p.3.
[250] ICO, 2024, Section 6 of Age Assurance for the Children's Codes. [Accessed 16 December 2024].
[251] ICO response to our May 2024 Consultation, p.5
[252] [✂]; Association of Police and Crime Commissioners response to our May 2024 Consultation, p.3; Big Brother Watch response to our May 2024 Consultation, pp.22-23; Burville, M response to our December 2023 Part 5 Consultation, pp.1-3; Collier D, response to our December 2023 Part 5 Consultation, pp.1-3; Free Speech Coalition response to December 2023 Part 5 Consultation, p.7; ; Fringe Dweller Productions response to our December 2023 Part 5 Consultation, pp.1-3; Global Network Initiative response to our May 2024 Consultation, pp.4-5; Mega Limited response to our May 2024 Consultation, p.14; Hutchison, A response to our December 2023 Part 5 Consultation, p 2-3; Jackson, EM response to our December 2023 Part 5 Consultation, p 2-3; ID Crypt Global response to December 2023 Part 5 Consultation, p.1; Name withheld 9 response to our December 2023 Part 5 Consultation, p.3; Mid Size Platform Group response to our May 2024 Consultation, p.3; Pinterest response to our May 2024 Consultation, p.12; Integrity Institute response to our May 2024 Consultation, pp.2-3; Northern Ireland Commissioner for Children and Young People (NICCY) response to May 2024 Consultation, p.31; Name Withheld 8 response to our December 2023 Part 5 Consultation, pp.2-3; Name Withheld 1 response to our December 2023 Part 5 Consultation, pp. 1-3; Name Withheld 2 response to our December 2023 Part 5 Consultation, pp.2-3; Name Withheld 3 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 4 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 5 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 6 response to our December 2023 Part 5 Consultation, pp.1-3; Safazadeh, S, response to our December 2023 Part 5 Consultation, pp.1-3; Shaw, A. response to our December 2023 Part 5 Consultation, pp.1-3; Warren A, response to our December 2023 Part 5 Consultation, pp.2-4; xHamster response to our December 2023 Part 5 Consultation, p.3; xHamster response to our May 2024 Consultation, p.2; 14 further confidential individual respondents to our December 2023 Part 5 Consultation, pp.1-4.

generally.[253] Some respondents expressed concern about the privacy implication of specific methods:

a) Free Speech Coalition and Inkbunny cited age estimation and/or age verification as particularly risky because the data they generate could be of particular value to hackers.[254] REPHRAIN highlighted that the risk of data misuse shows the need to sufficiently safeguard this data.[255] Meta suggested that requiring age verification on all services increases the number of providers holding this user data, who may then be targeted by hackers seeking to gain access to this data. They also highlighted that requiring age verification at account registration for all users may conflict with privacy principles of proportionality and data minimisation.[256] WhatsApp suggested that some age verification solutions may conflict with data protection principles such as data minimisation, purpose limitation, storage limitation, and security.[257]
b) ACT - The App Association argued that methods that rely on hard identifiers (e.g. photo-ID matching) are overly intrusive because they often contain more personal information than just a user's age.[258]
c) Open Rights Group raised concerns around the privacy risks associated with age verification.[259]

3.273 WhatsApp considered that the types of age assurance measures proposed by Ofcom are not the most privacy-preserving measures available for children's data.[260]

3.274 ACT - The App Association commented that there is currently no ideal way to conduct age assurance in a way that is both accurate and privacy preserving.[261]

3.275 In response to our December 2023 Part 5 Consultation, some respondents expressed concern about privacy risks in the specific context of pornography service providers implementing age assurance:

a) Free Speech Coalition suggested that the implementation of age assurance on pornographic websites may provide opportunities for extortion.[262] ID Crypt Global also highlighted that photo identification matching may provide an avenue for cyber criminals to capture information which could lead to identity theft and blackmail.[263] Big

[253] Big Brother Watch response to our May 2024 Consultation, p.22; Integrity Institute response to our May 2024 Consultation, pp.2-3.
[254] Free Speech Coalition response to Part 5 consultation, pp.5-7; Inkbunny response our May 2024 Consultation, p.12.
[255] REPHRAIN response to our May 2024 Consultation, p.14.
[256] Meta response to our May 2024 Consultation, p.15.
[257] WhatsApp response to our May 2024 Consultation, p.3.
[258] ACT - The App Association Response to our May 2024 Consultation, pp.2-3.
[259] Open Rights Group response to November 2023 Illegal Harms Consultation, p.6.
[260] WhatsApp response to our May 2024 Consultation, p.3.
[261] ACT - The App Association response to the May 2024 Consultation p.6.
[262] Free Speech Coalition response to Part 5 consultation, p.7.
[263] ID Crypt Global response to Part 5 consultation, p.3.

Brother Watch and a group of individual respondents also highlighted the risk of blackmail to more vulnerable communities.[264]

b) ID Crypt Global and StripChat also outlined the risk of bad actors where sites mimic the age verification processes of legitimate platforms to scam and defraud users through gaining their personal data.[265]

3.276 Yoti questioned the ICO's capacity to take referrals from Ofcom, where Ofcom has concerns, based on its written record, that a service provider has not complied with its obligations under data protection laws. It requested that Ofcom indicates how many services are in scope of Part 5 to understand how feasible this approach is.[266]

Stakeholders suggested changes to Ofcom's proposals regarding user privacy

3.277 5Rights argued that Ofcom should include 'privacy preserving' in the criteria, on the basis that this would mandate that services have privacy and security built into their processes.[267] The Age Check Certification Scheme suggested that providers should embed information security from the outset and throughout their lifecycle.[268]

3.278 5Rights stated that the criteria must include that age assurance must only use necessary information for establishing the age of the user and delete this data once it has confirmed age; not store data for other purposes or "aggressively" collect data; and ensure higher protection for children as per the standards of the ICO's Children's code. 5Rights also expressed concern that the criteria does not refer to the Children's code, which "the Act states that Ofcom must have regard to".[269]

3.279 Arcom was considering imposing at least one 'double blind' solution to better protect privacy.[270] A 'double blind' solution involves an age check being carried out by a third-party provider, and ensuring that: i) the third party provider is not able to identify the regulated service, for which the age check is being completed; and ii) the regulated service is not able to identify the user who is undergoing the age check.[271]

---

[264] Big Brother Watch response to our May 2024 Consultation, p.28; Burville, M response to our December 2023 Part 5 Consultation, p.5; Collier D, response to our December 2023 Part 5 Consultation, p.5; Hutchison, A response to our December 2023 Part 5 Consultation, p.6; Fringe Dweller Productions response to our December 2023 Part 5 Consultation, p.5; Jackson, EM response to our December 2023 Part 5 Consultation, p 5; Name Withheld 8 response to the our December 2023 Part 5 Consultation, p.5; Name Withheld 1 response to our December 2023 Part 5 Consultation, p.5; Name Withheld 2 response to our December 2023 Part 5 Consultation, p.5; Name Withheld 3 response to our December 2023 Part 5 Consultation, p.5; Name Withheld 4 response to our December 2023 Part 5 Consultation, p.5; Name Withheld 5 response to our December 2023 Part 5 Consultation, p.5; Name Withheld 6 response to our December 2023 Part 5 Consultation, p.9; Safazadeh, S, response to our December 2023 Part 5 Consultation, p.5; Shaw, A. response to our December 2023 Part 5 Consultation, p.5; Warren A, response to our December 2023 Part 5 Consultation, p.5; 14 further confidential individual respondents to our December 2023 Part 5 Consultation, p.5.

[265] ID Crypt Global response to our December 2023 Part 5 Consultation, p.3; StripChat response to our December 2023 Part 5 Consultation, p.5.

[266] Yoti response to our December 2023 Part 5 Consultation, p.18.

[267] 5Rights response to our December 2023 Part 5 Consultation, p.2.

[268] Age Check Certification Scheme response to the May 2024 Consultation, p.11.

[269] 5Rights response to our December 2023 Part 5 Consultation, p.6.

[270] Arcom response to our December 2023 Part 5 Consultation, p.5.

[271] LINC, 2022, Demonstration of a privacy-preserving age verification process [accessed 9 January 2025]

3.280 StripChat argued that Ofcom should assess age assurance providers with regard to the privacy safeguards they have instituted. They highlighted that the onus is on the age assurance service provider to ensure that personal data is securely stored.[272]

3.281 Yoti disputed the use of the word 'intrusive' in our May 2024 consultation to describe age assurance methods on the basis that it creates the perception that age assurance cannot meet data protection requirements.[273] Yoti noted that there are "data minimised" approaches available in the market, whereby via selective disclosure, only an age attribute such as "over 18", "13-17", or "under 18" is shared. Yoti argued that Ofcom should clarify when collecting the precise age of a user would be considered appropriate or inappropriate and urged Ofcom to clarify that service providers should limit data collection to what is necessary to determine if a user is a child and be transparent about this data collection.[274]

3.282 The Family Online Safety Institute outlined its view that "higher levels" of age assurance are more invasive (e.g. government ID or a credit card) and "lower forms" of age assurance (e.g. estimation technologies) are more privacy preserving but carry a higher margin of error. It stated that age assurance processes present a delicate trade off that must be carefully considered by regulators.[275]

3.283 Many respondents outlined the importance of Ofcom working with the ICO to clarify which age assurance methods are suitable for both the online safety and data protection regimes.[276] Meta suggested that it would be beneficial for Ofcom and the ICO to produce joint guidance on age assurance to allow providers to adapt their process for compliance.[277]

3.284 The Age Check Certification Scheme suggested that providers should proactively embed privacy into their age assurance systems from the outset. It argued that age assurance systems should have robust "fail safe mechanisms" to ensure that in the event of a system failure or malfunction that the service's functional, performance, privacy, security and acceptability characteristics are not compromised. This should include reverting to the safest default settings, stopping any processing and collection of data and not producing age assurance outputs in the event of a systems failure.[278] It also stated that users should be given sufficient and accessible information about what data will be shared between the age assurance provider and the content provider.[279]

3.285 Online Dating and Discovery Association and techUK argued that age estimation, when combined with other techniques in a layered or "waterfall" approach, can be less intrusive. They suggested that providers should start with less invasive methods and escalate to more stringent measures if necessary, in order to provide robust age assurance while respecting

[272] StripChat response to our December 2023 Part 5 Consultation, p.4.
[273] Yoti response to our May 2024 Consultation, p.28.
[274] Yoti response to our May 2024 Consultation, p.13 and p.31.
[275] Family Online Safety Institute response to our May 2024 Consultation, p.11
[276] 5Rights response to our December 2023 Part 5 Consultation, p.6; Microsoft response to our May 2024 Consultation, p.12; Open Rights Group response to November 2023 Illegal Harms Consultation, p.6; Yoti response to our May 2024 Consultation, p.28.
[277] Meta response to our May 2024 Consultation, p.15.
[278] Age Check Certification Scheme response to our May 2024 Consultation, pp.7-8.
[279] Age Check Certification Scheme response to our May 2024 Consultation, p.8.

user privacy.[280] The ICO suggested that we include an additional step in the case study in section 4 of the Part 5 Guidance to explain that services should provide a means for people to challenge age estimation or age verification results which they know to be inaccurate.[281] This suggestion relates to the data protection principle of accuracy. In the Commissioner's Opinion,[282] the ICO explains "people have the right to correct inaccuracies in their information which means you **must** consider any challenges to the accuracy." 5Rights and Integrity Institute argued that there needs to be a route to redress or appeal mechanism for age assurance when a user is incorrectly identified as a child.[283] The Age Check Certification Scheme similarly felt that relying parties should provide means for an individual to seek redress, and take responsibility for engagement with the age assurance provider on behalf of individuals.[284] However, Big Brother Watch suggest that even if redress is available, this would be retrospective and access is still blocked in the meantime.[285]

Our decisions

Relationship between our approach to highly effective age assurance and the UK's data protection regime

3.286 Regulated and enforced by the ICO, UK data protection law requires services to have privacy and security of data built into their processes.

3.287 As the bodies responsible for regulating data protection and online safety in the UK, the ICO and Ofcom demonstrated their shared commitment to protecting people online by publishing a joint statement in November 2022. The statement recognised that online safety and data protection interact in a variety of ways, including where age assurance is used. It set out our overall ambition to ensure coherence across online safety and data protection requirements and promote compliance with both regimes. Developing an aligned approach to the regulation of age assurance has been a priority for both organisations, and we will continue to work closely together as the online safety regime comes into force.

3.288 We have not amended the criteria to include a requirement around preserving privacy, because service providers and third-party age assurance solution providers operating in the UK or providing goods and services to individuals in the UK are already required to comply with the legal obligations established under the data protection regime. We agree that it is important that service providers have regard to user privacy when deciding on and implementing their age assurance processes, but it would not be appropriate or necessary to separately reflect requirements under data protection legislation in the criteria. Instead, we have referred to relevant ICO guidance in the Part 5 Guidance and the Part 3 HEAA Guidance.

---

[280] Online Dating and Discovery Association response to our May 2024 Consultation, p.6; techUK response to our May 2024 Consultation, pp.14-15.
[281] ICO response to our December 2023 Part 5 Consultation, p.7.
[282] Section 6.1.6 of the ICO's Opinion on Age Assurance. For more information on the right to rectification, see the ICO's 'A guide to individual rights'.
[283] 5Rights response to our December 2023 Part 5 Consultation, p.4; Integrity Institute response to our May 2024 Consultation, p.13.
[284] Age Check Certification Scheme (ACCS) response to our May 2024 Consultation, p.12.
[285] Big Brother Watch response to our May 2024 Consultation, p.31.

3.289 In particular, the UK GDPR requires that service providers, when implementing an age assurance method, collect the minimum amount of personal data required for the process, and do not retain any personal data collected by the method for longer than is needed. Service providers must not use personal data collected for the purpose of age assurance for any other incompatible purpose.[286] We have updated from paragraph 5.16 of the Part 5 Guidance and Section 5 of the Part 3 HEAA Guidance to make it clearer that all age assurance methods should follow a data protection by design approach[287] in order to comply with data protection legislation. As stated in the ICO's 'Guide to Lawful Basis', the lawful basis for processing will not apply if you can "reasonably achieve the purpose by some other less intrusive means, or by processing less data."[288] As such, service providers should use highly effective age assurance methods which are less intrusive and process the minimum amount of personal data needed.

3.290 In response to comments about navigating trade-offs between effectiveness and privacy of age assurance methods, we emphasise that compliance by service providers with both the online safety and the data protection regime is mandatory and should not be considered a trade-off. Where we have concerns that a provider has not complied with its obligations under data protection law, we may refer the matter to the ICO for consideration.

3.291 In response to Yoti's query about the feasibility of Ofcom referring cases to the ICO, we emphasise that consideration of these cases would be at the ICO's discretion.

"Double blind" solution

3.292 We have considered the point raised on the "double blind" approach (see paragraph 3.279 above) and we are of the view that service providers may consider the "double blind" approach to age assurance methods, which relies on an age check being carried out by a third party and shared in a privacy-preserving manner with the service that the user is attempting to access. Whilst it is likely not to be the only means of complying with both regimes, the "double blind" approach, which conceals both the identity of the user undergoing the age check and the service that the user is attempting to access, could be one means of achieving this, provided that the age check carried out by the third party is shown to be highly effective.

Risk to users from mishandling or abuse of personal data

3.293 We acknowledge concerns from a number of stakeholders that the implementation of age assurance carries certain risks, some of which are compounded in the context of access to pornographic content. This could include service providers mishandling users' personal data or, more worryingly, the risk of extortion or blackmail of users or vulnerable communities.

3.294 In respect of stakeholder comments about the risks of non-compliance with data protection law by service providers or third-party age assurance providers, we have addressed these issues at paragraph 3.290 above.

3.295 In relation to stakeholder comments about the risk of age-assurance related scams and fraud, we will continue our stakeholder engagement with the NCA and ICO to collaborate on

[286] Section 1.3 of the Information Commissioner's Opinion for Age Assurance.
[287] ICO, Data protection by design and by default.
[288] ICO, A guide to lawful basis.

how addressing these risks. We make clear in paragraph 5.11 of the Part 3 HEAA Guidance and paragraph 5.16 of the Part 5 Guidance that service providers have a duty to have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy. We would also encourage service providers to be clear in their communication with their users about the age assurance process and any third-party age assurance providers used so that they can have confidence when undergoing an age check (see further paragraph 4.90 on accessibility). This would include sharing clear and timely communications with their users about any changes to their service regarding its age assurance process to keep users safe and manage risk from bad actors to their services. We will also be engaging in public awareness campaigns to encourage adults to engage safely with legitimate age assurance processes.

On making reference to the ICO's Children's Code in the Part 5 Guidance

3.296 The ICO Children's code is designed for online services who are likely to be accessed by children, to ensure that children have the best possible access to online services while minimising processing data collection and use by default.

3.297 The ICO states that where a service provides an adult service and wishes to restrict access to children, if restricting access is done effectively (i.e. through the use of age assurance) so that children no longer represent a significant number of users, the code does not apply.[289] For this reason, we have not referenced the Children's code in the context of Part 5 service providers, who in all cases should be preventing children from accessing pornographic content, rather than making their service appropriate for child users. This was confirmed by the ICO in its response to our December 2023 Part 5 Consultation as the correct approach.[290]

3.298 In response to the ICO's suggestion, we have included an additional step in the illustrative case study in the Part 5 Guidance which recommends that a service provider should provide a means to challenge an inaccurate age estimation or age verification result in order to meet their requirements under the UK's data protection regime. Unlike for Part 3 where we have proposed user reporting and complaints measures under the draft Protection of Children Codes, Part 5 services are not required to have a complaints handling process for compliance with the Part 5 duties. However, we have included this step in the illustrative case study in the interests of showing a comprehensive picture of a typical user journey. As we state in both the Part 5 Guidance at paragraph 5.19 and Part 3 HEAA Guidance at 5.5, service providers should consult ICO guidance to understand how to comply with the data protection regime.

[289] ICO, 2024, Age Assurance for the Children's Codes.[accessed 28 December 2024].
[290] ICO response to our December 2023 Part 5 Consultation, p.3.

Principles for services to consider when designing or implementing age assurance that is easy to use

Our proposals

3.299 In the draft Part 5 Guidance and draft Part 3 HEAA Guidance, we proposed that service providers should consider the principle of accessibility, in order to ensure that their approach to age assurance is easy to use and works for all users, regardless of their characteristics or whether they are members of a certain group.[291] We suggested that providers should:

- Assess the potential impact that the chosen age assurance method(s) might have on users with different characteristics.
- Consider offering a variety of age assurance methods and allowing the user to choose which is most appropriate for them.
- Design the user journey through the age assurance process to be accessible for a wide range of abilities, including blindness, deafness, limited movement, and learning disabilities.

3.300 In the draft Part 5 Guidance and draft Part 3 HEAA Guidance, we also proposed that service providers should consider interoperability, defined as the ability for technological systems to communicate with each other using common and standardised formats. We suggested that providers should stay up to date with developments in interoperable age assurance methods and use these approaches to reduce the burden on the user where possible and appropriate for the service.

3.301 In the draft Part 3 HEAA Guidance, we further proposed that services should also consider the principle of transparency, namely the practice of disclosing relevant information so that others can make informed decisions. We stated that we consider it important that users are informed about the age assurance process before completing an age check. We also said that setting this information out clearly and accessibly in their terms of service will help services comply with the duties to include provisions in their terms of service specifying how children are to be prevented from encountering primary priority content that is harmful to children, and protected from encountering priority content that is harmful to children and non-designated content on their service.[292]

Summary of responses

3.302 In general, respondents agreed on the importance of considering accessibility and interoperability when designing an approach to age assurance.[293]

---

[291] Section 82(3) of the Act

[292] Section 12(9) and 12(13) of the Act.

[293] Barnardo's response to our December 2023 Part 5 Consultation, p.7; Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, p.6; CEASE response to our December 2023 Part 5 Consultation, p.5; ICO response to our December 2023 Part 5 Consultation, p.6; OpenID response to our December 2023 Part 5 Consultation, p.4-5; Te Mana Whakaatu Classification Office response to our December 2023 Part 5 Consultation, p.3; Verifymy response to our December 2023 Part 5 Consultation, p.6.

Interoperability

3.303 Some respondents cited the user experience benefits of an age assurance approach where a single age check can work across a range of services, so that a user only has to undergo an age check once.[294] Open Identity Exchange suggested that age restricted content providers should therefore seek age assurance providers, schemes or orchestrators that enable interoperability across sites, and that Ofcom should make portability of age assurance from one provider to another a requirement. One individual highlighted that interoperability should be in place prior to considering the implementation of age verification processes.[295]

3.304 Snap argued that Ofcom had not given due regard to interoperability and that none of the proposed methods are capable of being interoperable. They highlighted that taking an approach where the results of an age assurance check are shared across all of the affected services would result in a much lower cumulative cost and so would be a more appropriate and proportionate approach. Snap argued that interoperability reduces security risks associated with the collection of sensitive data. Interoperability will minimise age checks and can mean that age checks are carried out by companies with proven track records.[296]

3.305 xHamster also requested further clarification on interoperability. It asked for clarification surrounding whether sharing age assurance tokens between different companies would be accepted. It stressed the importance of Ofcom consulting with the ICO to provide more information on what constitutes acceptable processing.[297]

3.306 Mid Size Platform Group stated that it would welcome a commitment from Ofcom to outline its long-term plans and objectives with its approach to age assurance, based on their concerns that the UK risks being misaligned with international approaches. They also stated that they would welcome further efforts on the UK's digital identity project, led by DSIT, as a "viable and government endorsed solution to age assurance", and referenced that the EU is exploring similar solutions through the eIDAS system.[298]

Accessibility

3.307 The ICO stated that ensuring age assurance approaches are accessible will also support compliance with the first data protection principle (which requires processing to be lawful, fair and transparent). It also highlighted that the proposal that service providers should offer users a choice of several age assurance methods could have a privacy-enhancing impact, because reliance on a single method increases the risk of circumvention, and the associated lack of protection for children's data online.[299] This view was similarly voiced by Open Rights Group, who suggested that a choice of age assurance systems would allow consumers to choose methods with the best data protection, security and privacy.[300]

---

[294] [✂]; Open Identity Exchange response to our December 2023 Part 5 Consultation, p.5; Open ID Foundation response to our December 2023 Part 5 Consultation, pp,4-5.
[295] Elliott, R. response to our May 2024 Consultation, p.9.
[296] Snap response to our May 2024 Consultation, pp.16-17.
[297] xHamster response to our December 2023 Part 5 Consultation, p.8.
[298] Mid Size Platform Group response to our May 2024 Consultation, p.8.
[299] ICO response to our December 2023 Part 5 Consultation, p.6.
[300] Open Rights Group response to Illegal Harms Consultation, p.7.

3.308 Some respondents suggested that Ofcom make the consideration of accessibility mandatory, on the basis that some users may not be able to access services that require, for example, a credit card or government-issued documents.[301] The Canadian Centre for Child Protection suggested that if this is not mandated, and requires further cost to services, services are unlikely to implement this.[302] Yoti highlighted that Ofcom should include a section on inclusivity as well as accessibility for the core criteria of highly effective age assurance.[303] The Age Check Certification Scheme also recommend a criterion of inclusivity, giving examples of what steps a service could take to meet this criterion including using universal design principles, and abiding by standards such as the Web Content Accessibility Guidelines (WCAG).[304] [305]

3.309 iProov urged Ofcom not to take claims that people lack access to authoritative identity sources at face value, and instead undertake its own research. They highlight that as identity is a requirement for voting, it is proportionate and reasonable that those who wish to access adult content be required to prove their identity lawfully using authoritative and trusted identity verification, which can be managed in a convenient and privacy secure manner.[306]

3.310 Yoti highlighted the prevalence of passports and other identifiers for children, and proposed that Ofcom hold an industry workshop on the accessibility of hard identifiers.[307] One respondent cited UK government research[308] finding that up to 9% of adults may also not have access to sufficient photo identification,[309] with ACT - The App Association suggesting that this method is exclusionary for people who do not have or cannot use official age documentation.[310] Google also highlighted that people may not have access to credit cards or government issued IDs, and that this may be compounded by individuals from vulnerable or marginalised groups also not wanting to disclose this information.[311]

3.311 Yoti suggested that Ofcom reference specific accessibility standards e.g. the ICO's Children's code, the Hemingway system of 'grade level' or the Web Content Accessibility Guidelines (WCAG). Yoti also suggested that Ofcom should adopt a "co-production" approach to guidance by involving disabled persons at the earliest possible stage of conception of policies and guidance.[312]

---

[301] Common Sense Media response to our December 2023 Part 5 Consultation, p.5; Open Identity Exchange (OIX) response to our December 2023 Part 5 Consultation, p.5; Yoti response to our May 2024 Consultation, p.17.
[302] Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, pp.6-7.
[303] Yoti response to our December 2023 Part 5 Consultation, p.14 and our May 2024 Consultation, p.17.
[304] Age Check Certification Scheme response to our May 2024 Consultation, p.7.
[305] W3C, Web Content Accessibility Guidelines (WCAG) 2.1 [accessed 9 January 2025].
[306] iProov response to our December 2023 Part 5 Consultation, p.10.
[307] Yoti response to our May 2024 Consultation, p.21.
[308] The Cabinet Office, 2021. Photographic ID Research- Headline findings. [Accessed 9 January 2024]
[309] [✂]
[310] ACT - The App Association response to our May 2024 Consultation, p.3.
[311] Google response to our May 2024 Consultation, p.24.
[312] Yoti response to our December 2023 Part 5 Consultation, pp.14-15.

3.312 Yoti argued that users should be provided with a choice of age assurance options so they can choose their preferred method or have an alternative method to use if they wish to challenge an age assurance outcome.[313]

3.313 Integrity Institute raised a concern regarding the accessibility of age assurance technologies for people who do not fit into clear categories, such as someone whose name does not match their ID, and therefore may be restricted access.[314]

3.314 Two respondents highlighted that age assurance requires adults to share personal data with a service, which can act as a significant barrier to access.[315] xHamster highlighted that consequently the majority of adults who wish to protect their privacy will switch to non-compliant services that will not implement age assurance measures.[316]

Transparency

3.315 In response to our May 2024 Consultation, the Age Check Certification Scheme suggested that both age assurance service providers and content service providers should establish age assurance practice statements and make these publicly available.[317]

Our decision

Interoperability

3.316 In response to stakeholder comments about interoperability, we acknowledge that a highly effective age assurance approach that is reusable across a range of services has the potential to reduce user friction.

3.317 In response to stakeholder responses about portable age checks, in the Part 5 Guidance at paragraph 4.11 and the Part 3 HEAA Guidance at paragraph 3.6, we acknowledge the role of age tokens and emphasise that it remains the responsibility of the regulated service provider to ensure that the initial age check and the process to share this information with the regulated service (e.g. through age tokens) are highly effective.

3.318 It is for each service provider to determine which kinds of age assurance methods are most appropriate for its regulated service to meet its duties under the Act. As is made clear in both the Part 5 Guidance and the Part 3 HEAA Guidance, Ofcom is supportive of the principle of interoperability of age assurance methods. It is likely that solutions will emerge in the market in the future to minimise the burden on users and services; we have highlighted in the guidance a number of such initiatives that are in train. We therefore encourage service providers to stay up to date with emerging developments.

Accessibility

3.319 In the Part 5 Guidance and the Part 3 HEAA Guidance (paragraphs 4.66-4.67), we have updated the accessibility principle to reference the importance of explaining to users what the age assurance process is designed to do and how it works, and how service providers can

[313] Yoti response to our May 2024 Consultation, p.27.
[314] Integrity Institute response to our May 2024 Consultation, p.12
[315] [✂]; xHamster response to our December 2023 Part 5 Consultation, p.8.
[316] xHamster response to our December 2023 Part 5 Consultation, p.8.
[317] Age Check Certification Scheme response to the May 2024 Consultation, p.41.

have regard to this. This detail was originally included under the transparency principle in the draft Part 3 HEAA Guidance.

3.320 We have also updated the guidance under the accessibility principle in the Part 5 Guidance to align with the Part 3 HEAA Guidance. This has reduced the level of detail for conciseness, but the substantive steps that we suggest service providers should consider remain the same.

3.321 With regard to stakeholder suggestions that we make the consideration of accessibility mandatory, the Act does not specifically impose any duties on services to ensure they make their age assurance processes accessible to any particular standard or for particular user groups. Instead they require age assurance to be highly effective at correctly determining whether or not a particular user is a child and, as discussed above, we have already reflected the need to ensure that age assurance methods avoid or minimise bias and discriminatory outcomes in our fairness criterion above. Given this, we have decided not to include accessibility in our above-mentioned four criteria that age assurance must fulfil to be highly effective. However, we are clear in the guidance that it is an additional principle we expect service providers to consider with a view to ensuring that adults are not unduly prevented from accessing legal content and children are prevented from encountering content which is harmful to them. We expect services to consider accessibility not just in the context of specific methods but for the purposes of the entire age assurance process they implement. One method may not be accessible to all, but when supplemented by alternative methods this can create an accessible age assurance process.

3.322 In relation to respondents' concerns about the risk that collection of personal data for age assurance creates an access barrier, we acknowledge that all methods of age assurance will inevitably involve the processing of personal data of individuals (including children unless they are dissuaded from entering any when they are asked to do an age check). In line with data protection requirements, service providers must implement their age assurance processes in a way which minimises the amount of personal data which may be processed or retained, so that it is no more than necessary to ensure it works effectively. Both the Part 5 Guidance and the Part 3 HEAA Guidance make clear that service providers should consult ICO guidance when implementing age assurance to understand how to comply with the data protection regime, including its guides to data minimisation and other data protection principles.[318]

Transparency

3.323 The Age Check Certification Scheme suggested that third party age assurance providers, as well as service providers, should keep a record of their age assurance process and make this publicly available. Our Part 5 Guidance sets out the record-keeping duties for Part 5 services. Part 3 services are also subject to separate record keeping duties which are covered under our Children's Access Assessment Guidance, discussed in section 5 of this document, and

[318] ICO, Principle (c): Data minimisation. [accessed 22 March 2024]. For an overview of each principle, see the ICO's guide to the data protection principles.

Ofcom's Record Keeping and Review Guidance.[319] Ofcom does not have the power to compel third party services not regulated under the Act to keep records.

3.324 As part of the process of aligning the Part 5 Guidance and the Part 3 Guidance, we have removed transparency as a standalone principle in the Part 3 HEAA Guidance, as we considered it redundant and duplicative. Instead, we have dealt with the points that had been covered in that section of the draft guidance in the following ways:

a) **We have updated the accessibility principle** to reference the importance of explaining to users what the age assurance process is designed to do and how it works, and how service providers can have regard to this, as explained above.
b) **We have moved reference to draft Codes measures**. In the draft Part 3 HEAA Guidance, we proposed that having regard to the principle of transparency could help service providers to comply with proposed measures related to i) terms of service and ii) reporting and complaints in the draft Protection of Children Codes.[320] We have summarised the interactions between the Part 3 HEAA Guidance and the Protection of Children Codes in paragraphs 2.5-2.9 of the Part 3 HEAA Guidance. As we explain, we will publish the final Protection of Children Codes in April 2025, and will update the guidance with references to the final Code as appropriate, including to reflect any changes to the wording of the relevant Codes measures.
c) **We have removed duplicative reference to the transparency principle under data protection legislation**, because it is covered under Section 5: Privacy and data protection of the Part 3 HEAA Guidance (paragraph 5.7).

Other general stakeholder comments on Ofcom's approach to highly effective age assurance

Our proposals

3.325 We stated that it is for each service provider to determine which kinds of age assurance methods are most appropriate for its regulated service to meet its duties under the Act.

3.326 We stated that we would expect to see that, when determining which age assurance method(s) to implement, service providers have satisfied themselves that the age assurance process as a whole fulfils each of the criteria. In doing so, we recognised that there may be trade-offs in how well individual age assurance methods perform against each of the criteria. We stated that it is the provider's responsibility to decide which trade-offs are appropriate to achieve the outcome that the overall age assurance process is highly effective at determining whether or not a particular user is a child.

[319] Ofcom, Protecting people from illegal harms online: Record-Keeping and Review Guidance, published 16 December 2024.
[320] See A10.71 and A10.73 of the Draft Guidance on Highly Effective Age Assurance.

Summary of responses

Level of detail provided in the guidance

3.327 Some respondents argued that the draft guidance lacked sufficient specificity or detail. TechUK felt that the guidance did not give a granular definition of highly effective age assurance.[321] Kooth Digital Health requested further guidance on what highly effective age assurance involves in order to prevent a "patchy landscape" where providers assess themselves.[322] Match Group commented that the criteria for highly effective age assurance are relatively vague.[323]

3.328 Other respondents argued that the guidance was too prescriptive. Mobile Games Intelligence Forum suggested that the guidance applies an overly prescriptive approach to what is highly effective and suggested that Ofcom take a more flexible approach.[324] Match Group warned that there will be unintended consequences unless a more flexible and pragmatic approach to age assurance is taken.[325] Meta highlighted that there is no one-size-fits-all solution to age assurance, and Ofcom must take a flexible approach to age assurance.[326]

3.329 Microsoft suggested that the guidance should provide more detail on how external vendors can provide appropriate certainty to multiple customers that meets the requirements of the UK's regime.[327]

3.330 Some respondents expressed support for the four criteria we proposed for determining whether an age assurance process is highly effective.[328] Another respondent expressed support for considering the four criteria as well as other criteria such as privacy and proportionality.[329] For example, the Age Check Certification Scheme argued that to understand whether age assurance is highly effective it should be assessed on the basis of more than just a simple classification of its accuracy.[330]

Assessing and monitoring effectiveness

3.331 One respondent argued that the expectation that service providers should assess the effectiveness of age assurance methods in order to satisfy themselves that their approach is compliant is unreasonable and unrealistic because they do not have the necessary expertise or capacity to do so.[331] Another respondent queried how providers are supposed to be able to select between different age assurance solutions.[332]

---

[321] techUK response to our May 2024 Consultation, p.3.
[322] Kooth Digital Health response to our May 2024 Consultation, p.10.
[323] Match Group response to the May 2024 Consultation, p.2.
[324] Mobile Games Intelligence Forum response to our May 2024 Consultation, pp.1-2.
[325] Match Group response to our May 2024 Consultation, p.3.
[326] Meta response to our May 2024 Consultation, p.16.
[327] Microsoft response to the May 2024 Consultation, p.11.
[328] NEXUS response to the May 2024 Consultation, p.14; Association of Police and Crime Commissioners response to the May 2024 Consultation, pp.3-4.
[329] [✂]
[330] Age Check Certification Scheme response to our May 2024 Consultation, p.2.
[331] [✂]
[332] Name Withheld 9 response to our December 2023 Part 5 Consultation, pp.1-2.

3.332 The Scottish Government recognised that services are required to assess the effectiveness of their age assurance, but also suggested that Ofcom should monitor this too.[333]

3.333 Yoti recommended that Ofcom "mandate independent third-party certification or assessment providers to test the effectiveness of age assurance methods and processes", on the basis that this would ensure that service providers "receive accurate information about their systems".[334]

3.334 Global Network Initiative recommended that Ofcom should develop and incorporate an assessment process to identify and mitigate risks associated with age assurance systems. They added that it would be important to exercise transparency with such assessments to help academics, civil society organisations and users better understand how services are addressing risks, and to allow them to hold Ofcom accountable.[335]

3.335 TikTok recommended that Ofcom clarify that services should self-assess whether their age verification is "highly effective" on the basis of internal statistics, for example through comparing the performance of the age assurance tools against performance targets that the service has set based on Ofcom's guidance as to what constitutes highly effective age assurance.[336]

3.336 Canadian Centre for Child Protection and iProov suggested that Ofcom should provide additional guidance on how providers should identify which trade-offs are or are not appropriate when considering highly effective age assurance.[337]

3.337 Ingenium Biometric Laboratories Limited suggested that greater clarity could be provided for services in how to approach the robustness criterion. They suggested it was unclear whether there was a role for independent audit and certification and independent empirical laboratory testing in ascertaining the robustness of a method.[338]

3.338 Some respondents commented on the importance of service providers ensuring that their approach remains highly effective on a continuous basis. The Children's Commissioner for England recommended that Ofcom include an obligation for service providers to report on the implementation and effectiveness of the measures.[339]

3.339 Common Sense Media recommended that Ofcom make clear its expectations that service providers should stay abreast of new age assurance methods and technologies and implement them in a reasonably timely manner.[340]

---

[333] The Scottish Government response to the May 2024 Consultation, p.3.
[334] Yoti response to our May 2024 Consultation, p.8.
[335] Global Network Initiative response to our May 2024 Consultation, p.12.
[336] TikTok response to our May 2024 Consultation, p.6.
[337] Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, p.3; iProov response to the May 2024 Consultation, p.5.
[338] Ingenium Biometric Laboratories Limited response to our May 2024 Consultation, p.8.
[339] Children's Commissioner for England response to the May 2024 Consultation, p.54.
[340] Common Sense Media response to our December 2023 Part 5 Consultation, p.3.

Consideration of proportionality

3.340 We also received comments about proportionality. In response to our December 2023 Part 5 Consultation, Yoti argued that Ofcom should create proportionality as a central criterion.[341] Yoti suggests that "fully verifying a user's age, rather than estimating whether a user is above or below an age threshold, should come as a last resort and only where it is proportional to do so".

3.341 On the other hand, the Online Safety Act Network argued that the Part 5 age assurance duty is not subject to proportionality considerations (although they accepted that Ofcom's approach as a regulator should be guided by the principle of proportionality).[342]

3.342 We also received a number of responses to our May 2024 Consultation calling for a risk and proportionality-based approach to age assurance. These comments relate largely to the application of highly effective age assurance, as defined through measures AA1-AA6 of the draft Protection of Children Codes and will therefore be addressed in our Protection of Children Statement in April 2025.

3.343 Free Speech Coalition argued that the draft Part 5 Guidance places full liability onto service providers, which they consider exceeds the requirements of the legislation. They stated that the law does not say that service providers must verify and take responsibility for the technical accuracy, robustness, reliability, and fairness of tools that they did not create.[343]

Our decisions

Level of detail provided in the guidance

3.344 We acknowledge responses from stakeholders around the level of detail provided in the draft guidance. Responses were mixed: some stakeholders argued that there was a lack of specificity, whilst others considered the draft guidance to be excessively prescriptive. Having considered stakeholder feedback, we have concluded that the division of responses received reflects the balance we have endeavoured to strike in our approach and have not made any substantive changes.

3.345 With regard to requests from techUK and Kooth Digital Health for more detail on the definition of highly effective age assurance, we have maintained our four criteria but clarified in the guidance that services can use methods other than those included in the list of methods that are capable of being highly effective, including wide system-level age assurance. Further to consideration of responses, we have taken steps to further align our Part 5 guidance and Part 3 HEAA guidance to ensure there is a common approach and to avoid uncertainty. Further, we consider that our decision to publish non-statutory guidance on Part 3 HEAA in January 2025 should increase clarity and help service providers to comply with their duties.

3.346 We disagree with respondent suggestions that our guidance is too prescriptive. As set out in the sub-section 'Decision regarding Ofcom's overall approach', we believe the level of detail

[341] Yoti response to our December 2023 Part 5 Consultation, p.20
[342] Online Safety Act Network response to our December 2023 Part 5 Consultation, p.6.
[343] Free Speech Coalition response to our December 2023 Part 5 Consultation, p.8.

in our approach is appropriate and provides flexibility as technology continues to develop at pace. We are also clear in the Part 5 Guidance at paragraph 4.8 and the Part 3 HEAA Guidance at paragraph 3.3 that it is for the service provider to determine which age assurance method(s) to use in order to implement an age assurance process that is appropriate to meet its duties under the Act.

3.347 By providing a non-exhaustive list of kinds of age assurance that have the potential of being highly effective and detailed criteria to apply when implementing that age assurance, we have provided services with a clear indication of how to comply with their duties, while leaving flexibility to implement an age assurance process that best suits their business.

3.348 We have refined our guidance on navigating trade-offs, to make it more explicit that whilst we recognise that different kinds of age assurance may perform more strongly in some of the criteria than others, we expect service providers to satisfy themselves that the age assurance process as a whole fulfils each of the criteria, and ultimately meets the duty to ensure that children are not normally able to access pornographic content (Part 5 services) or are prevented from encountering harmful content (Part 3 services).

Assessing and monitoring effectiveness

3.349 We have carefully considered stakeholder feedback regarding assessment and monitoring of effectiveness. We agree with stakeholder responses that it is important that service providers assess the effectiveness of their age assurance processes on an ongoing basis.

3.350 In response to Yoti's call for Ofcom to mandate independent third-party certification or testing of the effectiveness of age assurance processes, we maintain that our approach is neutral as to who develops or makes available the highly effective age assurance solutions. Our guidance is clear that service providers are responsible for ensuring the effectiveness of their age assurance process, however, they can rely on information supplied by a third-party. If service providers rely on a third-party age assurance provider this will likely require them to obtain relevant information from that third-party provider which provides them with appropriate evidence that the age assurance being implemented is highly effective.

3.351 Service providers may choose to rely on testing carried out by a third-party such as an independent auditor or a certification or standards body. We have updated our guidance at paragraph 4.26 of the Part 5 Guidance and paragraph 4.5 of the Part 3 HEAA Guidance to make clear that where we refer to testing as a means of supporting compliance with the criteria, metrics could be derived from the providers' own internal testing (if feasible), from the testing that third party age assurance providers have done, or from testing by an independent third party. Where testing has been carried out by third parties, service providers should understand what tests have been conducted and the metrics which have been used to measure the results.

3.352 We have updated our guidance at paragraph 4.27 of the Part 5 Guidance and paragraph 4.60 of the Part 3 HEAA Guidance to make explicit that services may use certification against an appropriate standard or scheme to demonstrate compliance with their duties. However, regulated services must be satisfied that meeting the certification standards allows them to meet the criteria for highly effective age assurance.

3.353 As set out in paragraph 3.108, we have expanded the reference to the UK Digital Identity and Attributes Trust Framework in the Part 5 Guidance at paragraph 4.27 and the Part 3 HEAA Guidance at paragraph 4.6. Using a service certified against the trust framework (or

any other standard or scheme) is not an automatic means of compliance, but it may help to evidence that a service provider has had regard to the four criteria to ensure that its approach is highly effective. With regard to concerns about service providers' expertise or capacity to assess effectiveness of age assurance methods, a register of certified services is published on GOV.UK, helping individuals and businesses to choose trustworthy services.

3.354 With regard to Ingenium Biometric Laboratories Limited's comment about the robustness criterion, we welcome advances in consistent, comparable testing methodologies and recognise a potential role for independent audit and certification and independent empirical laboratory testing in ascertaining the robustness of a method.

3.355 With regard to stakeholder feedback around service providers ensuring their approach remains highly effective over time, our guidance is clear that services must undertake regular monitoring and measurement. In our guidance on the reliability criterion at paragraph 4.69 of the Part 5 Guidance and paragraph 4.46 of the Part 3 HEAA Guidance, we state that service providers should ensure that there is regular monitoring and measurement of the key performance indicators of the system as part of fulfilling the reliability criterion, for example, by noting any trends of inaccurate age estimations and/or a rise in complaints/appeals. We also suggest at paragraph 4.43 of the Part 5 Guidance and paragraph 4.21 of the Part 3 HEAA Guidance that providers should ensure their age assurance processes are reviewed and updated periodically to determine whether newer, more effective technologies and testing practices may provide a higher level of technical accuracy.

3.356 Ofcom will monitor compliance and, where we have concerns that service providers are not meeting their duties, we may carry out more detailed assessments of services' age assurance processes. As Ofcom is required to produce a report about the use of age assurance under section 157 of the Act, we will be gathering evidence on how age assurance is being used to comply with the duties in the Act. As part of this report, we will assess factors that have prevented or hindered the effective use of age assurance, which we expect to include any risks associated with age assurance methods per the comment from Global Network Initiative. We will include such evidence in that report when we publish it in 2026.

Consideration of proportionality

3.357 In response to the stakeholder feedback calling for Ofcom to incorporate proportionality as a criterion into the concept of highly effective age assurance, we reiterate that service providers have a duty under the Act to implement highly effective age assurance in order to prevent children from encountering pornographic content and, for Part 3 services, other forms of harmful content. We consider "highly effective" to be a single standard of effectiveness that must apply in all cases covered by the relevant provisions in Part 5 and Part 3 of the Act, as explained in the Part 5 Guidance and Part 3 HEAA Guidance and Annex 1 of this statement. In developing our approach to highly effective age assurance we have been mindful of our duties (as set out in Annex 1). We have considered proportionality as part of our proposed approach to highly effective age assurance, including by giving service providers flexibility in implementing a kind of highly effective age assurance process which is suitable for their service and user base. We have therefore not amended the criteria to include proportionality.

3.358 In response to the Free Speech Coalition's point on liability, as set out in para 3.98 in the sub-section on 'Age assurance at the app store, device, or operating system (OS) level', the

Act makes clear that the responsibility for preventing children from accessing pornographic content falls firmly on the part of the service provider where Part 5 applies. We explain how service providers are expected to assess any third-party age assurance methods they may use from para 3.350 under sub-section 'Assessing and monitoring effectiveness'. As such, we do not consider that the Part 5 Guidance exceeds the requirements of the legislation.

3.359 We consider our approach to highly effective age assurance to be proportionate overall and we assess the likely impacts of our decisions in Annex 2. We have not assessed the impact of the proposed age assurance measures in our draft Protection of Children Code for user-to-user services in this document, but we will do so when we finalise our decisions in our April Protection of Children Statement.

Next steps

3.360 Providers of Part 5 services are required to comply with their duties under the Act, including the requirement to use highly effective age assurance, from 17 January 2025 when the duties commence.[344]

3.361 Part 5 providers should refer to Section 4 of this statement, as well as final Part 5 Guidance, to understand how they can meet all the requirements of the Act relating to the scope of Part 5.

3.362 Providers of Part 3 services must carry out children's access assessments by 16 April 2025 at the latest. Our final position on children's access assessments is set out in Section 5 of this statement. All Part 3 services should refer to our final Children's Access Assessments Guidance as they take immediate steps to comply with their duties. Where Part 3 service providers are already using age assurance, they should also refer to the Part 3 HEAA Guidance to understand whether it is highly effective age assurance.

3.363 We will publish our final Protection of Children Codes and guidance in April 2025. At that point, providers of user-to-user services likely to be accessed by children will need to assess the risks they pose and take action to protect them in line with our Protection of Children Codes – which may include using highly effective age assurance to prevent children from accessing harmful content. Part 3 services should also consult the Part 3 HEAA Guidance to understand how to implement highly effective age assurance. We will update the Part 3 HEAA Guidance as appropriate in line with our decisions on the Protection of Children Codes.

[344] See the Online Safety Act 2023 (Commencement No. 4) Regulations 2024

4. Additional guidance on aspects applicable only to Part 5 services

Ofcom is required to produce and publish guidance for Part 5 services to assist them in complying with their duties under Part 5 of the Act ("Part 5 Guidance"). In addition to the duties relating to implementing highly effective age assurance, as discussed in Section 3, they also include record-keeping duties. In this section, we explain how we have considered stakeholder responses that we received on other aspects of our draft Part 5 Guidance and set out our final position on these aspects of the Part 5 Guidance. This includes guidance on the scope of Part 5, record keeping, and our approach to enforcement of the Part 5 duties.

We have largely maintained our proposed approach but have made some minor changes to the draft Part 5 Guidance, primarily to improve clarity for service providers:

- We have expanded the guidance on scope to make it easier for services to determine whether they should comply with the Part 5 duties, including additional examples. We have explained how Generative AI services may fall into scope of the Part 5 duties and clarified how services should make determinations about whether they have 'links with the United Kingdom'.

- Regarding the record-keeping duties, we have added guidance to emphasise the need to comply with data protection law when implementing age assurance, and also clarified that service providers do not need to record the outcome of every age check in their written records.

- We have not updated our approach to assessing compliance within the Part 5 Guidance. Any enforcement action will be taken in line with our Online Safety Enforcement Guidance which was published in December 2024.[345] Services should consider it to understand how Ofcom will approach enforcement of duties imposed on regulated providers under the Act.

Introduction

4.1 As set out in Section 3 of this statement, the concept of highly effective age assurance is consistent for Part 3 and Part 5 services, as reflected in the Part 5 Guidance and the Part 3 HEAA Guidance.

4.2 In this section, we deal with the other areas that are specific to the Part 5 Guidance, in addition to the age assurance duties, namely:

- **the scope of Part 5:** assessing whether a service is in scope of the Part 5 duties;

[345] The final version has now been published here: Protecting People from illegal harms online: online safety enforcement guidance. Published 16 December 2024

- **the record-keeping duties:** considering how service providers can keep a written record and produce a publicly available statement setting out how they have complied with their duties, including how providers may have regard to the importance of protecting users from breaches data protection legislation; and
- **assessing compliance with age assurance and record-keeping duties:** the principles that we will normally apply when determining whether a service provider has complied with its duties and where we are likely to consider that it has not complied.

Our proposals

Scope of internet services regulated as Part 5 services

4.3 The statutory duties imposed by section 81 of the Act only apply to providers of an internet service falling within the description in section 80(2), that is to say the following conditions must be satisfied for an internet service to fall within the scope of Part 5 of the Act:

a) regulated provider pornographic content is published or displayed on the service ('condition 1');
b) the service is not out of scope of Part 5 or exempt ('condition 2'); and,
c) the service has links with the United Kingdom ('condition 3').

4.4 In our draft Part 5 Guidance, we provided an overview of each of these conditions which determine whether a regulated service is in scope, with reference to the relevant statutory conditions. We also provided some high-level examples to assist service providers in understanding how these definitions might apply.

The record-keeping duties

4.5 The following duties relating to record-keeping are imposed on providers of Part 5 services:

a) A duty to make and keep a written record in an easily understandable form of:

i) the kinds of age verification or age estimation used, and how they are used;[346] and
ii) the way in which the service provider, when deciding on the kinds of age verification or age estimation and how they should be used, has had regard to the importance of protecting UK users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a regulated service (including, but not limited to, any such provision or rule concerning the processing of personal data);[347] and

b) A duty to summarise the written record in a publicly available statement, so far as the record concerns compliance with the duty set out in section 81(2), including details

[346] Section 81(4)(a) of the Act.
[347] Section 81(4)(b) of the Act.

about which kinds of age verification or age estimation a service provider is using and how they are used.[348]

4.6 In the draft Part 5 Guidance, we set out information that providers of Part 5 services should consider including about their age assurance processes. In particular, we proposed that they should include in their written records how they have had regard to each of the criteria and principles set out in the draft Part 5 Guidance and their reasons why they consider that the age assurance process they are using fulfils each of them.

4.7 In the draft Part 5 Guidance, we also provided examples of how service providers can record that they have had regard to user privacy. We explained that we would continue to work closely with the ICO on the privacy aspects of the Part 5 duties once they come into force.

4.8 Regarding summarising the written record in a publicly available statement, we proposed that service providers should clearly explain to users how the age assurance process works and why it is necessary. We also proposed that service providers should make the statement available to the general UK public in an easy to find area of the website, for example, in the section at the top (header) or bottom (footer) of the home page, where users can typically find site contact details and navigation links, or on the service's landing page. We further proposed that service providers should provide the summary alongside any explanatory text on how the age assurance works when a user begins the age assurance process, so that they can read this before completing the age assurance check.

4.9 The draft Part 5 Guidance also included examples of circumstances where a service provider has not complied with the record-keeping duties, these included where the provider has not updated the written record to ensure it remains current.

Assessing compliance with age assurance and record-keeping duties

4.10 In the draft Part 5 Guidance, we also set out an overview of our general approach to enforcement under the Act, including the principles that we will consider when determining whether a service provider has complied with the duties. We also directed services to the Online Safety Enforcement Guidance ("OS Enforcement Guidance"), which sets out the procedures Ofcom will follow where we suspect non-compliance with the obligations that apply to service providers under the Act.[349] In particular, the draft Part 5 Guidance made it clear that we intended to follow the procedures in the OS Enforcement Guidance when deciding whether and how to take enforcement action against non-compliance with Part 5 duties.

[348] Section 81(5) of the Act.

[349] In the draft guidance we referred to the draft online safety enforcement guidance. The final version has now been published here: Protecting People from illegal harms online: online safety enforcement guidance. Published 16 December 2024

Guidance on scope of the Part 5 duties

4.11 As noted in paragraph 4.3 above, the Act sets out three conditions that must be satisfied for a service provider to fall within the scope of Part 5 of the Act:

a) regulated provider pornographic content is published or displayed on the service ('condition 1');
b) the service is not out of scope of Part 5 or exempt ('condition 2'); and,
c) the service has links with the United Kingdom ('condition 3').

4.12 We did not receive any stakeholder feedback on our proposals in relation to condition 2 specifically and we have therefore decided to adopt our position on that condition. In the remainder of this sub-section, we set out and address stakeholder feedback in relation to conditions 1 and 3.

Condition 1: Regulated provider pornographic content is published or displayed on the service

Definition of a Part 5 service

Our proposal

4.13 In the draft Part 5 Guidance, we explained what we think that the expression "published or displayed by the provider of the service" means in the context of section 79 of the Act.

4.14 The circumstances in which 'pornographic content' (the meaning of which we discuss below) will be treated as "published or displayed" on a service are set out in section 79(6)(a) of the Act, and they include circumstances where the pornographic content:

- is only visible or audible to users as a result of interacting with content that is blurred, distorted or obscured (for example, by clicking on the content) but only where the pornographic content is present on the service;
- is embedded on the service; or
- is generated on the service by means of an automated tool or algorithm in response to a prompt by a user and is only visible or audible to that user (no matter for how short a time).

4.15 To assist providers of Part 5 services in better understanding the Act, we provided some examples of where content will be treated as published or displayed on a service by the provider of the service. They were:

- "a service provider has designed and provided interactive games featuring pornographic imagery on its service, we might consider that this content has been published or displayed by the provider"; and
- "a service provider is responsible for live-streaming pornographic video content on its service, this would also be an example of where we would likely consider the provider to be subject to Part 5."

4.16 In the draft Part 5 Guidance, we also explained that there may be instances where online services include some pornographic content which falls in scope of Part 3 and some pornographic content which falls in scope of Part 5. To illustrate, we gave the example that, while tube sites are often U2U services that are predominantly comprised of user-generated pornographic content, a provider of a tube site may itself make some pornographic content

available on that site.[350] Where a provider of such a service (which otherwise predominantly comprises user-generated content) publishes or displays pornographic content on its site, or someone else does so on its behalf, that pornographic content will be within scope of the Part 5 duties, unless otherwise exempt.

Summary of responses

4.17 Some respondents suggested that the distinction between Part 3 and Part 5 could be made clearer in the Part 5 Guidance: two respondents suggested that it is unclear how content that falls under Part 3 and Part 5 and appears on the same site will fall within the scope of different parts of the Act.[351] Conversely, One ID suggested that the guidance is clear that provider generated content is Part 5 and user generated content is Part 3, and that providers who supply both kinds will need to comply with both.[352]

4.18 The Age Verification Providers Association and Verifymy suggested that tube sites should be covered under Part 5 rather than Part 3.[353] The Age Verification Providers Association suggested that paid-for advertisements could be interpreted to apply to much of the content on tube sites, e.g. an adult site places examples of their content on these sites and a pay-per-click model is in place when users visit or subscribe to the producer's site.[354] One respondent commented that the case of tube sites shows how the distinction between Part 3 and Part 5 can be confusing.[355]

4.19 The Free Speech Coalition suggested that simplifying the language where possible and incorporating more examples from business models being used in the adult industry would be helpful for the clarity of this section of the guidance.[356]

Our decisions

4.20 We have edited the structure of this section of the Part 5 Guidance to improve clarity and readability for service providers. We have also given additional examples to clarify the types of circumstances in which we might judge that a provider of a service is publishing or displaying pornographic content within the meaning of Part 5. These examples are designed to make clear that pornography that is made by either an individual (for example, a creator) or a studio, and then uploaded onto an online service controlled or run by that individual or studio may be considered as being published or displayed by the provider of the service. However, this is intended to be an illustrative example only, and the examples we have included in the Part 5 Guidance are non-exhaustive and the Part 5 duties will apply in other circumstances where the applicable statutory tests are met.

---

[350] The BBFC defines tube services as free-to-access video-sharing platforms "which allow users to upload and share videos with the public," in BBFC, 2023, Functionality of Online Pornography Services. A BBFC research report for Ofcom, p.10.
[351] [✂]; Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, pp.1-2.
[352] One ID response to our December 2023 Part 5 Consultation, p.1.
[353] Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.1; Verifymy response to our December 2023 Part 5 Consultation, p.2.
[354] The Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.5.
[355] [✂]
[356] Free Speech Coalition response to our December 2023 Part 5 Consultation, p.3.

4.21 We have also removed the example of livestreaming pornographic video content. Since the publication of the draft Part 5 Guidance, we have engaged with the adult industry to further understand the nature of control of content. In our engagement with adult services, we have learned that livestreaming is a much more common functionality on U2U services, meaning our original example of "livestreaming" may confuse service providers. It remains possible that content on a livestreaming service is considered to be published or displayed by the provider of the service, where the provider of the online service exercises editorial control over the nature, selection or presentation of livestreamed content (for example, where a content creator livestreams the creation of pornographic content onto a service that they control or run themselves). With instances of livestreamed provider pornographic content being very rare, we have judged this is an unhelpful example to use in the guidance and have therefore removed it.

4.22 In response to Age Verification Providers Association and Verifymy's comments about tube sites, we set out in the Part 5 Guidance that it is possible for Part 5 content to be present on a predominantly U2U service (i.e. a service caught by Part 3 which predominantly comprises user-generated content), for example on a tube site. This would be where some content is published by or on behalf of the provider of the tube site. An example may be a premium or subscription section of the tube site with provider content. We also recognise that there may be commercial agreements between sites that could impact the assessment of whether content is being uploaded by or on behalf of the provider. It is for the service provider to assess their service by reference to the Act and Ofcom guidance to determine the duties it is subject to. In relation to paid-for advertisements, the Act expressly excludes these from scope of the Part 5 duties.[357] It is for providers to assess whether or not content is in scope of the Part 5 duties or constitutes a paid-for advertisement, as defined in section 236 of the Act.

4.23 Whether a service or content is classified as Part 3 or Part 5, all services allowing pornographic content must have highly effective age assurance in place to protect children by July 2025. At that point, there will be no difference in practice whether a service or a piece of content is classified as Part 5 or a Part 3 U2U service.

Meaning of pornographic content

Our proposal

4.24 In the draft Part 5 Guidance, we explained that "pornographic content" is defined by the legislation as "content of such a nature that it is reasonable to assume that it was produced solely or principally for the purpose of sexual arousal."[358] We provided more context in the draft Part 5 Guidance by referring to the BBFC R18 classification to explain that pornographic content might include content that falls into this classification.[359]

[357] Section 79(3) and (5) of the Act
[358] Section 236(1) of the Act.
[359] R18 is a special classification, which can only be shown to adults in specially licensed cinemas and can only be supplied to adults in licensed sex shops. BBFC, R18 rating. [accessed 9 January 2025].

Summary of responses

4.25 The Children's Commissioner for England supported Ofcom's use of the BBFC's definition of pornographic content.[360] The Christian Institute suggested that Ofcom should make clear that material rated '18' by the BBFC may also be included in scope.[361]

4.26 Some respondents argued that the definition of 'pornographic content' is not clear enough.[362] During stakeholder engagement with pornographic services on this topic, a number of service providers raised questions about whether seductive content, meaning content that is suggestive or sexual in nature, but does not meet the definition of pornographic content, would need to be behind a highly effective age assurance process, given its principal purpose could be argued as sexual arousal. Examples included sex scenes from films, sexually suggestive music videos, or sexually suggestive images which do not show actual nudity but could be considered as only intended for the purposes of sexual arousal. One respondent questioned whether seductive content or content provided only as a preview, that is not pornographic, would need to be behind highly effective age assurance.[363]xHamster argued that age assurance should only be required before initially accessing adult content, and not before accessing the entire platform which hosts both pornographic and non-pornographic content.[364]

4.27 The Scottish Government suggested that Ofcom should make clear whether cartoon images and CGI pornographic content falls in scope of Part 5.[365]

Our decisions

4.28 It is a matter for Parliament, not Ofcom, to define the meaning of "pornographic content" in section 236(1) of the Act, as cited above, and, ultimately, it is for the courts to interpret its meaning.

4.29 We note, however, that a key statutory test to determine whether certain content[366] is pornographic (or not) is to consider whether it is reasonable to assume that it was produced 'solely or principally' for the purpose of sexual arousal. Whether content has been produced either solely or principally for the purpose of sexual arousal is likely to be dependent on the nature of the content itself, having taken the relevant contextual factors into account, rather than the intent of the uploading user or any viewer of it. In response to stakeholder comments about seductive content, a service provider should determine, informed by the broader factual context, whether the content has been produced for the sole or principal purpose of sexual arousal, such that it may be deemed to be pornographic content.

---

[360] Childrens Commissioner for England response to our December 2023 Part 5 Consultation, p.18.
[361] Christian Institute response to our December 2023 Part 5 Consultation, pp.1-2.
[362] Christian Institute response to our December 2023 Part 5 Consultation, pp.1-2; Name Withheld 9 response to our December 2023 Part 5 Consultation, p.1.
[363] Name withheld 9 response to our December 2023 Part 5 Consultation, p.1.
[364] xHamster response to our December 2023 Part 5 Consultation, p.10.
[365] Scottish Government response to our December 2023 Part 5 Consultation, p.1.
[366] By "content", the Act refers to anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description: see section 236(1).

4.30 Further guidance on pornographic content will be included in the Harms Guidance for Part 3 services. Ofcom is required to produce guidance on content, or kinds of content, that is harmful to children in relation to duties for user-to-user and search services under Part 3 of the Act.[367] We published a draft version of this guidance in April 2024,[368] and will publish the final version in April 2025, taking into consideration the comments we have received.

4.31 Pornographic content does include artificial images, such as images produced by generative artificial intelligence, and we have expanded the Part 5 Guidance at paragraph 3.7 to make this point clear.

4.32 It is correct that, as The Christian Institute highlighted, some pornography classified with an '18' rating by the BBFC may be in scope.[369] Our Part 5 Guidance makes clear that content of a strong sexual nature that seeks to sexually arouse or stimulate, that would not fall in scope of the R18 classification, may also be treated as pornographic content for the purposes of Part 5. It is for service providers to determine whether content was produced principally for the purpose of sexual arousal.

Generative AI

Our proposal

4.33 Our draft Part 5 Guidance explained that the Act specifies that the definition of regulated provider pornographic content includes pornographic content published or displayed on the service by means of:

- a software or an automated tool or algorithm applied by the provider or a person acting on behalf of the provider, or
- an automated tool or algorithm made available on the service by the provider or a person on behalf of the provider.[370]

4.34 In light of those provisions, we set out in our draft Part 5 Guidance that the meaning of "published or displayed by the provider on its internet service" in the context of Part 5 includes pornographic content generated on the service by a generative artificial intelligence (Generative AI) tool or an algorithm in response to a prompt by a user. The guidance explained that, according to other provisions in the Act, the provider of the relevant internet service is treated as the entity or person with control of, and making available, the tool or algorithm in question.[371]

Summary of responses

4.35 Many respondents expressed support for the inclusion of AI generated pornographic content in the scope of Part 5.[372]

---

[369] BBFC, R18 rating. [accessed 9 January 2025].
[369] BBFC, R18 rating. [accessed 9 January 2025].
[369] BBFC, R18 rating. [accessed 9 January 2025].
[370] See section 79(6)(a)(iii)) of the Act.
[371] Section 226(15) of the Act.
[372] 5Rights response to our December 2023 Part 5 Consultation, p.3; Barnardo's response to our December 2023 Part 5 Consultation, p.3; [✂]; Canadian Centre for Child Protection response to our December 2023 Part

4.36 Some respondents suggested that the draft Part 5 Guidance could be clearer in its explanation of how Generative AI services fall in scope of Part 5.[373] 5Rights called for greater clarity as to "how this guidance will apply to all Generative AI spaces that host technology which allow users to create pornography."[374] They outlined several cases in which the scope was not clear, including in regard to "services which provide the models for users to create this content, but do not necessarily publish the content on the service" and "nudify apps". 5Rights highlighted the scenario of "websites which do not exclusively allow for the creation of gen-AI pornography, but supply models for the creation of all types of content" and suggested we could be clearer in our draft Part 5 Guidance about how these are treated. The Canadian Centre for Child Protection gave the example of an open-source tool for AI text-image where the primary use and function is not to create pornographic content, but certain prompts result in the creation of pornographic content. They queried how this type of tool would be considered regarding Part 5.[375]

4.37 Respondents also shared their concerns about the rise of Generative AI pornographic content in general, and especially where it is used to create sexual content without consent.[376]

Our decisions

4.38 Where Generative AI tools have U2U functionalities – such as where a site or app includes a Generative AI chatbot that enables users to share text, images or videos generated by the chatbot with other users – they may fall in scope of the duties on U2U services under Part 3 of the Act. This includes, for example, services with 'group chat' functionality that enables multiple users to interact with a chatbot at the same time – whether this chatbot functionality is the main feature of the service, or is just part of a bigger service such as a social media platform. This is set out in our open letter published in November 2024 to online service providers operating in the UK about how the Act will apply to Generative AI and chatbots.[377] This section focuses on services that provide Generative AI tools which may fall in scope of Part 5, rather than Part 3.

4.39 It is clear that a range of stakeholders are concerned about the risk of harm to children from pornographic content which is produced by Generative AI. We have provided additional information, at paragraphs 3.19-3.24 of the Part 5 Guidance, to help providers of Generative

---

5 Consultation, p.3; CEASE response to our December 2023 Part 5 Consultation, p 2; CARE response to our December 2023 Part 5 Consultation, p 3; Name Withheld 5 response to our December 2023 Part 5 Consultation, p.1; Nexus response to our December 2023, Part 5 consultation, pp.1-2; One ID response to our December 2023 Part 5 Consultation, p.1; Scottish Government response to our December 2023 Part 5 Consultation, p.2; Verifymy response to our December 2023 Part 5 Consultation, p.1; Welsh Government response to our December 2023 Part 5 Consultation, p.1; Yoti response to our December 2023 Part 5 Consultation, pp.2-3.

[373] 5Rights response to our December 2023 Part 5 Consultation, p.3; Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, p.3.

[374] 5Rights response to our December 2023 Part 5 Consultation, p.3.

[375] Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, p.3

[376] Barnardo's response to our December 2023 Part 5 Consultation pp.3-4; Nexus response to our December 2023 Part 5 Consultation pp.1-2; Name Withheld 5 response to our December 2023 Part 5 Consultation, p.5; Te Mana Whakaatu Classification Office response to our December 2023 Part 5 Consultation, pp.1-2.

[377] Ofcom, 2024, Open letter to UK online service providers regarding Generative AI and chatbots

AI tools assess when they are in scope of the Part 5 duties. We explain that a Generative AI tool that is provided with the intention of allowing users to generate pornographic content would be in scope of the Part 5 duties, assuming the 'UK links' test is met.

4.40 The Part 5 Guidance also clarifies that, where a service provides a Generative AI tool that is not designed to create pornographic content but is still capable of doing so, and the service provider does not wish the tool to be in scope of the Part 5 duties, they would be advised to implement effective safeguards to prevent pornography from being generated in order to ensure they are outside the scope of the Part 5 duties. To that end, we have included an illustrative list of safeguards in the Part 5 Guidance. These safeguards could include, for example:

- the use of keyword blockers that prevent certain 'prompts' being entered into Generative AI models (in this case, terms associated with pornography);
- content classifiers that can detect potentially pornographic content and prevent it from being shown to users;
- removing pornographic content from the datasets used to train Generative AI models;
- red teaming Generative AI models to evaluate the strength of these and other safeguards and, identifying where further improvements need to be made. For more information on red teaming see our discussion paper on Red Teaming for Generative AI Harms.[378]

4.41 We note in the Part 5 Guidance that services that offer Generative AI functionalities need to secure the outcome of preventing the creation of pornographic content. The effectiveness of safeguards may vary significantly depending on the deployment context and how they are implemented. Therefore, it is the responsibility of providers of Generative AI tools to explore the full range of safeguards at their disposal and to assess for themselves the effectiveness of those safeguards in preventing their Generative AI tools from producing pornographic content, if they do not want to fall in scope of Part 5 of the Act.

4.42 We have also made clear in the Part 5 Guidance that including a provision in the terms of service for a Generative AI tool that prohibits the tool being used to create pornographic content would not secure the outcome of preventing this type of content being produced, and therefore would not be enough to ensure that a service is not caught by the scope of Part 5.

'Nudify' services

4.43 While many Generative AI tools are used to create synthetic pornographic content that features no real individuals, others have been designed deliberately to create 'deepfakes' that falsely portray real people in sexual contexts. These tools are often known as 'nudify services'. A recent Ofcom paper, *Deepfake Defences*, identified that the use of such tools is increasingly commonplace, with as many as 10 percent of children aged 13-16 saying they had either directly experienced or knew of someone who had experienced being featured in fake nude images or videos.[379] Where nudify services allow users to share generated content

[378] Ofcom, 2024, Red Teaming for GenAI Harms
[379] Ofcom, 2024. Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes

with other users of the service, the service could be considered to be a regulated U2U service and therefore the provider of the service would need to comply with the Part 3 duties, as applicable, including the illegal harms duties of the Act.[380] This would mean, among other things, that the service provider would need to take proportionate steps to prevent users encountering priority illegal content, and remove illegal content when they become aware of it (for example because it amounts to intimate image abuse or child sexual abuse material). Where nudify services do not fall into scope of Part 3 (i.e. because the service has no user sharing functionality), they may fall in scope of Part 5. This would be the case where the deepfake nude content being generated is pornographic content within the meaning of the Act.

Condition 3: The service has links with the United Kingdom

Our proposal

4.44 A service has links with the UK for the purposes of Part 5 of the Act if either of the following conditions is met in relation to the service:

- the service has a significant number of UK users, or
- the UK forms one of the target markets for the service, or the only target market.[381]

4.45 The draft Part 5 Guidance explained that the Act does not define what is meant by a significant number of UK users for the purposes of considering whether the service has links with the UK. We stated that service providers should be able to provide evidence to explain their judgement of what they have considered to be a significant number, especially if they think they do not have a significant number of UK users.

Summary of responses

4.46 CARE and Barnardo's suggested that section 80(4) of the Act should be interpreted in the widest possible terms, and that any site that UK users can use to access pornography should be deemed as having 'links to the UK'.[382]

4.47 Several respondents argued that the guidance on 'significant number' of UK users should be clearer.[383] This included a suggestion that the Part 5 Guidance should set a clearer threshold for the number of UK users that a service would need to have in order to be in scope of Part 5,[384] and the suggestion that it be made clearer whether a service is required to determine

[380] The key duties on regulated U2U services relating to illegal harms are set out in sections 9 and 10 of the Act. See the December 2024 Statement for more details, in particular the Overview of Illegal Harms which summarises the relevant illegal harms and duties on services relating to illegal harms.
[381] Section 80(4) of the Act.
[382] Barnardo's response to our December 2023 Part 5 Consultation, p.3; CARE response to our December 2023 Part 5 Consultation, p.1.
[383] 5Rights response to our December 2023 Part 5 Consultation, p.3; Barnardo's response to our December 2023 Part 5 Consultation, p.3; Canadian Centre for Child Protection response to our December 2023 Part 5 Consultation, p.2; Christian Institute response to our December 2023 Part 5 Consultation, p.2, StripChat response to our December 2023 Part 5 Consultation, p.3; Yoti response to our December 2023 Part 5 Consultation, p.2.
[384] StripChat response to our December 2023 Part 5 Consultation, pp.2-3, Yoti response to our December 2023 Part 5 Consultation, p.2.

the significance of their UK-based visitor numbers in relation to the total population of the UK or in comparison to their global user base.[385] Some respondents were concerned that a lack of clarity would lead to services with small user bases ruling themselves out of scope of Part 5 and children would continue to be able to access pornography.[386]

4.48 5Rights and Yoti suggested that Ofcom should follow the ICO's approach to "likely to be accessed by children" from the ICO's Childrens code.[387] [388] 5Rights suggested that Ofcom should follow the ICO's approach of setting a "low bar" for the definition of "significant number" in the context of the Children's code, in order to maintain regulatory alignment.

4.49 5Rights and StripChat questioned the reliability of user-number measurement.[389] StripChat suggested that there can be a disparity between user-numbers reported by publicly available measurement tools and those collected by regulated services themselves.[390] 5Rights suggested that services are not usually transparent about their user-number data.[391]

Our decisions

4.50 We have decided not to include a numerical threshold for a "significant number of United Kingdom users" in the Part 5 Guidance. The Act does not empower Ofcom to set any form of legally binding numerical threshold for the purposes of the statutory test in the Act, nor does it require Ofcom to provide guidance on what Ofcom considers is meant by a 'significant number'. We considered whether suggesting an indicative threshold above which we would be likely to consider services to be in scope would assist services in complying with their Part 5 duties. We remain of the view that what is meant by a significant number will depend on the context of the service in question, and therefore indicating a single numerical threshold above which Ofcom would be likely to consider a service to be in scope would not be appropriate at this time. Service providers will need to undertake their own assessment of whether or not the services they provide meet one or both of the applicable statutory conditions.

4.51 However, in order to assist service providers to understand how Ofcom is likely to expect them to approach this assessment, we have decided to expand the Part 5 Guidance at paragraph 3.31 to reflect our view that the concept of "significant number of UK users" is likely to mean that the number of UK users on the service is material in the context of the service in question, rather than the number of UK users of the service necessarily being a large or substantial number.

---

[385] Christian Institute response to our December 2023 Part 5 Consultation, p.2; Yoti response to our December 2023 Part 5 Consultation, p.2.
[386] 5Rights response to our December 2023 Part 5 Consultation, p.3; Barnardo's response to our December 2023 Part 5 Consultation, pp.2-3.
[387] ICO, 'Likely to be accessed' by children – FAQs, list of factors and case studies.
[388] 5Rights response to our December 2023 Part 5 Consultation, p.3; Yoti response to our December 2023 Part 5 Consultation, p.2.
[389] 5Rights response to our December 2023 Part 5 Consultation, p.3; StripChat response to our December 2023 Part 5 Consultation, p.3.
[390] StripChat response to our December 2023 Part 5 Consultation, p.3.
[391] 5Rights response to our December 2023 Part 5 Consultation, p.3.

4.52 We do not consider that the UK links test is intended to exclude services from the scope of the Part 5 duties simply because they have relatively small user bases, as this would not align with the purpose of the Part 5 duties which is to secure that children in the UK should not normally be able to encounter regulated provider pornographic content. We therefore suggest that providers of Part 5 services should err on the side of caution when assessing whether they have a significant number of UK users and are in scope of Part 5, taking independent legal advice as needed.

4.53 To assist service providers, we have also given additional guidance at paragraph 3.34 of the Part 5 Guidance on factors that may indicate that the UK is a target market for a service, including where a service:[392]

- is designed for UK users;
- is promoted or marketed toward UK users;
- generates revenue from UK users either directly (e.g. via subscriptions or sales) or indirectly (e.g. through advertising to UK users, including people or organisations);
- includes functionalities or content that is tailored for UK users; or
- has a UK domain or provides a UK contact address and/or telephone contact number.

4.54 Only one of the two conditions (significant number of UK users or UK as a target market) needs to be met for a service to have links with the UK. This means that, even if a service does not have a significant number of UK users, it may be in scope if they have the UK as a target market. This is set out at paragraph 3.31 of the Part 5 Guidance, which we have updated to clarify this point. Conversely, a service may be in scope if it has a significant number of UK users but the UK is not a target market.

Guidance on record-keeping duties

Our proposals

4.55 In Section 5 of the draft Part 5 Guidance, we proposed steps that service providers should take when making and keeping a written record and summarising it in a publicly available statement for the purposes of complying with their record-keeping duties under Part 5 of the Act. In particular, we stated that our proposed guidance on record keeping follows the approach in the draft guidance on Record Keeping and Review, published as part of our November 2023 consultation on illegal harms and now published in final form in December 2024.[393]

4.56 We also set out in the draft Part 5 Guidance the information that we proposed service providers should consider including about their age assurance process in their written

[392] These factors are also mentioned in Ofcom's Online Regulation Checker: https://ofcomlive.my.salesforce-sites.com/formentry/RegulationChecker.

[393] November 2023 Consultation, Annex 6: Guidance on record keeping and review. This has now been updated in the December 2024 Illegal Harms Statement, Record keeping and review guidance, published 16 December 2024.

records and publicly available statement, including how they can show that they have had regard to each of the criteria and principles when implementing their age assurance process.

4.57 We further signposted service providers to ICO guidance,[394] to help them understand how to have regard to the importance of protecting user privacy to comply with the data protection regime, and provided examples of how service providers could keep a record of having done so.

4.58 We also set out examples of circumstances where we are likely to consider that a service provider has not complied with the record-keeping duties.

Summary of responses

4.59 Stakeholders generally expressed support for our guidance related to the record-keeping duties,[395] with some respondents citing that the requirement to make a statement publicly available would help to ensure transparency for users and accountability for service providers.[396]

4.60 Open Identity Exchange and Yoti acknowledged that keeping a record of the results of individual age checks was not a requirement but said this was not made clear.[397] Yoti suggested that as a result, providers may unnecessarily keep a record of information such as a user's age or full date of birth.[398] 5Rights expressed concern that service providers will have to record a great deal of likely sensitive data as a result of the written record duties.[399]

4.61 One respondent argued that the guidance section on written record duty related to privacy could be expanded to include the considerations of the "privacy-trade-offs" that a provider's choice of age assurance method could mean for a user.[400] Yoti stated that providers should only retain the meta-data about the age check, rather than a user's date of birth.[401]

4.62 Several respondents argued that the written records should be used to record the effectiveness of the age assurance process. They suggested that providers should record the outcome of their age assurance method to show that it is highly effective at preventing children from normally being able to encounter pornography.[402]

---

[394] The Opinion can be found at ICO, Children's code guidance and resources. [accessed 9 January 2025]
[395] Children's Commissioner for England response to our December 2023 Part 5 Consultation, pp.19-20; One ID response to our December 2023 Part 5 Consultation, p.4; Te Mana Whakaatu Classification Office response to our December 2023 Part 5 Consultation, p.4; Veridas response to our December 2023 Part 5 Consultation, p.13; Welsh Government response to our December 2023 Part 5 Consultation, p.2.
[396] Te Mana Whakaatu Classification Office response to our December 2023 Part 5 Consultation, p.4.
[397] Open Identity Exchange response to our December 2023 Part 5 Consultation, p.6; Yoti response to our December 2023 Part 5 Consultation, p.17.
[398] Yoti response to our December 2023 Part 5 Consultation, p.17.
[399] 5Rights response to our December 2023 Part 5 Consultation, p.8.
[400] Yoti response to our December 2023 Part 5 Consultation, p.17.
[401] Yoti response to Illegal Harms Consultation, p.8.
[402] 5Rights response to our December 2023 Part 5 Consultation, p.2; Barnardo's response to our December 2023 Part 5 Consultation, pp.8-9; Centre to End All Sexual Exploitation (CEASE) response to our December 2023 Part 5 Consultation, p.5.

4.63 One stakeholder highlighted that service providers that use third party age assurance solutions should be able to cross reference records held by the third party to prevent these records being duplicative.[403]

4.64 Free Speech Coalition called for Ofcom to provide a template demonstrating compliance.[404] One respondent queried where providers should place their publicly available statement; for example, if it is placed at the footer of a webpage this may have accessibility issues, particularly for mobile phone users.[405]

4.65 xHamster argued that some responsibilities, such as ensuring that the method used has been tested on diverse data, should lie with third-party age assurance providers who have in-depth knowledge of their processes, and that Ofcom should reassess the allocation of these responsibilities.[406]

Our decisions

4.66 It is the responsibility of the service provider to demonstrate via their written record how they meet the duty. Given the potential complexity and diversity of deployment contexts and age assurance processes, we have not provided a template to demonstrate compliance with the duties. It is for providers to determine how best to present their records in line with the design of their service. We have taken this approach to afford service providers flexibility, so long as they include all relevant information, and therefore we do not think it is appropriate to be unduly prescriptive. Provided the written record is durable, accessible, easy-to-understand, up-to-date and written in clear simple language as recommended in the Part 5 Guidance, then it may be appropriate for a service provider who uses a third-party age assurance provider to cross reference records held by its chosen third-party age assurance provider to avoid these records being duplicative.

4.67 In response to the comment that the responsibility for compliance with data protection law should lie with third-party age assurance providers, we highlight that should a service provider choose to use a third-party age assurance solution; it is for the service provider and that third party to identify their respective roles and obligations under data protection law.[407] The Part 5 Guidance is intended to help service providers comply with their requirements to keep written records of the way in which they have had regard to privacy when deciding on the kind of age assurance measures to use. Part 5 services may need to make enquiries of third-party age assurance providers to ascertain how privacy and data protection law are being considered in the process of implementing age assurance on the Part 5 service.

4.68 Regarding stakeholder comments on the written record duty related to privacy and data protection, we consider that service providers can and should implement age assurance and comply with their record-keeping duties in a way that minimises the amount of personal data which may be processed or retained, beyond what is required for implementing the age

[403] The Age Verification Providers Association) response to our December 2023 Part 5 Consultation, p.10.
[404] Free Speech Coalition response to our December 2023 Part 5 Consultation, p.8.
[405] [✂]
[406] xHamster response to our December 2023 Part 5 Consultation, pp.8-9.
[407] See the ICO Guidance on controllers and processors for more information.

assurance process, so that the amount of data collected is no more than necessary. We expect providers to comply with data protection law, with further information given in paragraphs 5.20 to 5.25 of the Part 5 Guidance. We address the comment regarding "privacy trade-offs" in paragraph 3.285 of this statement. Please see the sub-section on 'Privacy, data protection and security concerns with highly effective age assurance' from paragraph 3.262 of this statement where we discuss data protection in more detail.

4.69 In response to comments from Open Identity Exchange, Yoti and 5Rights, the duties in the Act requiring written records to be kept do not require service providers to keep a record of the outcome of individual age checks. We have clarified this at paragraph 5.12 of the Part 5 Guidance. Where providers choose to retain results of individual age checks, this must be done in a manner which is compliant with data protection law. The UK GDPR sets out seven key principles which apply to the processing of personal data; this includes having a lawful basis for doing so and ensuring that the data is not kept longer than is needed.[408]

4.70 In response to comments suggesting that service providers should record the effectiveness of their age assurance process, we emphasise that the record-keeping duties do require services to record the kinds of age verification or age estimation used, and how they are used.[409] The Part 5 Guidance is clear that service providers should record "how each method or combination of methods fulfils the criteria and principles set out in Section 4",[410] therefore services should record their assessment of the accuracy, robustness, reliability and fairness of their age assurance process.

Additional changes to guidance on the Part 5 record-keeping duties

4.71 In our December 2024 statement 'Protecting people from illegal harms online' ("December 2024 statement"), we published updated guidance on Record Keeping and Review.[411] We have made the following change to our Part 5 Guidance to align with the updated version of this Record Keeping and Review Guidance:

a) At paragraph 5.13 of the Part 5 Guidance, we have changed the retention period that we expect for record keeping. As explained at paragraph 4.24 of our statement on the Record Keeping and Review Guidance, in order to align with other regulatory regimes, such as the EU's Digital Services Act (DSA), we recommend a three-year retention period for record keeping, rather than the five years previously stated. As explained at paragraph 4.29 of our statement on the Record Keeping and Review Guidance, this should still allow for records to be available if retrospective problems are identified. It

[408] The seven principles are set out in Article 5 of the UK GDPR and elaborated on in the context of age assurance in The Commissioner's Opinion on Age Assurance at section 6.1.5 on Data Minimisation and 6.1.7 on Storage Limitation. For completeness, see also the ICO's A guide to the data protection principles.
[409] Section 81(4)(a) of the Act.
[410] Guidance on highly effective age assurance and other Part 5 duties
[411] December 2024 Illegal Harms Statement, Record keeping and review guidance, published 16 December 2024.

should also ensure that records are available for providers to show how they have responded to the evolution of risks over time.[412]

4.72 We have also made the following minor changes to align with the original proposals from the Record Keeping and Review Guidance, as set out at paragraph 4.25 of our statement on the Record Keeping and Review Guidance:

- At paragraph 5.5 of the Part 5 Guidance, in order to align with paragraph 2.1 of our final Record Keeping and Review Guidance, we now state that "records should be durable, accessible, easy to understand, and up-to-date". This wording has also been reflected in the Overview of the Guidance and in Figure 5.1.
- At paragraph 5.8 of the Part 5 Guidance, in order to align with paragraph 2.4 of our final Record Keeping and Review Guidance, we have clarified that, where it is not reasonably practicable for the written records to be kept in English, the records must be capable of being translated into English.

Assessing compliance with age assurance and record-keeping duties

Our proposals

4.73 In our draft Part 5 Guidance, we set out an overview of our general approach to enforcement under the Act, including the principles that we will consider when determining whether a service provider has complied with the duties.

4.74 The draft Part 5 Guidance explained that the Act gives Ofcom the power to take enforcement action, including imposing financial penalties of up to £18 million, or 10% of qualifying worldwide revenues (whichever is greater), where we find that service providers have failed to comply with their Part 5 duties.[413] We explained in the draft Part 5 Guidance that Sections 4 and 5 of the guidance provide the analytical framework Ofcom would intend to apply when assessing whether the Part 5 duties have been met and examples of where we are likely to consider that a regulated service has not complied.

4.75 The draft Part 5 Guidance also explained that, when assessing compliance, we will act in accordance with our general duties, including our duty to have regard to our regulatory principles of transparency, accountability, proportionality, consistency and ensuring that regulatory action is targeted only at cases which require it.[414]

4.76 We signposted services to our draft OS Enforcement Guidance, which set out the procedures we proposed to follow where we suspect non-compliance with the obligations that apply to service providers under the Act.[415] We made clear in the draft Part 5 Guidance that we will

[412] Ofcom, Protecting people from illegal harms online: Volume 1, Chapter 4: Record-Keeping and Review Guidance, published 16 December 2024.
[413] Paragraph 4, Schedule 13 to the Act.
[414] Section 3(3)(a) of the 2003 Act.
[415] This guidance has now been published in its final form here: Protecting People from illegal harms online: online safety enforcement guidance. Published 16 December 2024.

follow the procedures in the OS Enforcement Guidance when deciding whether and how to take enforcement action against non-compliance with Part 5 duties.

Summary of responses

4.77 Two respondents expressed support for Ofcom's approach to enforcement,[416] another praised Ofcom's transparency but urged Ofcom to enforce quickly.[417]

4.78 The Scottish Government emphasised the need for quick and robust enforcement.[418] Some respondents expressed concern that Ofcom's approach to enforcement would not be adequately robust.[419] They suggested that under VSP regulation enforcement action was taking place too slowly. CEASE disagreed with Ofcom's approach of engaging first with services.[420] StripChat suggested that firms lacking a tangible presence in the UK may be less likely to comply with age assurance requirements, but that prompt enforcement action should still be taken.[421]

4.79 Some respondents highlighted the risk that user traffic would move from sites that have implemented age assurance to those that have not.[422] They used examples of this happening in Germany, France and certain US states to support the argument that the loss of user base could be such an existential threat to pornography services that service providers may see choosing to not comply and investing in legal defence as a better option than implementing age assurance.[423]

4.80 Respondents suggested that enforcement would need to be swift, robust and applied equally to the whole sector to reduce the risk of users moving from sites that have implemented age-assurance to those that have not.[424] StripChat argued that without a scalable method for enforcing compliance with age verification requirements, platforms are left with the option to either comply or ignore these requirements, leaving a vast number of websites unchecked and accessible by children.[425] xHamster explained that if services of all sizes are not forced to comply at the same time users will move from compliant to non-compliant sites, meaning that children will continue to not be protected from

[416] Brown, N. response to our December 2023 Part 5 Consultation, pp.4-5; Veridas response to our December 2023 Part 5 Consultation, p.13.
[417] Children's Commissioner for England response to our December 2023 Part 5 Consultation, p.20.
[418] Scottish Government response to our December 2023 Part 5 Consultation, p.3.
[419] Baroness Benjamin response to our December 2023 Part 5 Consultation, p.3; CEASE response to our December 2023 Part 5 Consultation, p.6; CARE response to our December 2023 Part 5 Consultation, pp.5-6, Christian Institute response to our December 2023 Part 5 Consultation, p.5; Lord Bethell response to our December 2023 Part 5 Consultation, pp.3-4; Yoti response to our December 2023 Part 5 Consultation, p.18.
[420] CEASE response to our December 2023 Part 5 Consultation, p.6.
[421] StripChat response to our December 2023 Part 5 Consultation, p.6.
[422] The Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.10; Barnardo's response to our December 2023 Part 5 Consultation, p.9; xHamster response to our December 2023 Part 5 Consultation, p.3.
[423] Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.10; Aylo response to our December 2023 Part 5 Consultation, p.2.
[424] Age Verification Providers Association response to our December 2023 Part 5 Consultation, p.10; Yoti response to our December 2023 Part 5 Consultation p.18.
[425] StripChat response to our December 2023 Part 5 Consultation, p.2.

pornography.[426] One respondent cited that following legislative changes in Louisiana, users moved to non-compliant sites that also do not protect user safety or moderate content.[427] xHamster also argued that age assurance will increase 'bounce rates',[428] meaning that compliant services will move down in search rankings, making non-compliant sites easier to find.[429]

4.81 iProov stated that its primary concern is that Ofcom's proposed guidelines "create conditions whereby the market is incentivised to embrace a weak solution today, knowing that enforcement against erroneous decisions is unlikely, creating a pull against adopting more robust solutions which provide for trusted verification that a user is provably an adult."[430]

Our decision

4.82 We have decided that it is unnecessary to make any substantive changes to our approach to assessing compliance following consideration of stakeholder responses that we received on these enforcement-related aspects.

4.83 Any enforcement action will be taken in line with our OS Enforcement Guidance,[431] which sets out our administrative priority framework for how we decide which cases to pursue and the processes we will follow when taking formal enforcement action.

4.84 In light of respondents' comments about quick and robust enforcement, we have removed the wording that suggests that we operate with a bias against intervention in the final version of the OS Enforcement Guidance.[432] We refer to the statutory language in respect of our duty to have regard to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent, and targeted only at cases in which action is needed; and any other principles appearing to Ofcom to represent best regulatory practice. We have made clear that, in terms of enforcement action, our approach is to take action only where it is proportionate and appropriate, but with a willingness to intervene firmly, promptly and effectively when required.

4.85 Regarding the implications for protection of children from our enforcement approach, Ofcom has a duty under the Act to have regard to the need for a higher level of protection for children than adults, and this is factored in throughout our administrative priority framework. The risk of harm to children will be a key consideration when determining how urgently we will take action and what course of enforcement action is most appropriate for services failing to comply with their Part 5 duties.

---

[426] xHamster response to our December 2023 Part 5 Consultation, p.9.
[427] Aylo response to our December 2023 Part 5 Consultation, p.2.
[428] 'Bounce rate' is a metric used in web traffic analysis to measure the percentage of visitors who leave a website after viewing only one page.
[429] xHamster response to our December 2023 Part 5 Consultation, p.9.
[430] iProov response to our December 2023 Part 5 Consultation, p.1.
[431] This guidance has now been published in its final form here: Protecting People from illegal harms online: online safety enforcement guidance. Published 16 December 2024.
[432] See paragraph 3.28 of Protecting people from illegal harms online: Volume 3 Transparency, trust and other guidance, published 16 December 2024.

4.86 With regard to stakeholder responses about the risk of users migrating to non-compliant sites, we have a range of non-statutory tools which we may use in response to a potential compliance concern, alongside our statutory powers to open investigations and take formal enforcement action (including imposing financial penalties), which may result in services coming into compliance sooner than through formal action. This may include sending warning letters and/or accepting commitments or assurances to remedy compliance concerns. Additionally, working with the industry through supervisory engagement and broader outreach work is a critical element of our work to promote compliance, to ensure that the sector is aware of their duties and the steps they need to take to comply. This will be balanced against the need to take swift action against serious breaches, and the importance of protecting children from harm. We have shown through our VSP regime how the application of a combination of statutory and non-statutory tools for enforcement can drive compliance with duties to protect children from pornography.[433]

4.87 We expect services to have already started preparing for the duties coming into force and have regularly published information on our website to help them understand how they can do so.[434] We have also been engaging with a range of service providers, including providers of smaller services and pornography services, to help them understand the new rules. This includes:

- engaging with pornography services directly and bodies who have online pornography services as members, like the Free Speech Coalition and the Association of Sites Advocating Child Protection (ASACP);
- attending international adult industry conferences to promote understanding of the Act;
- publishing guidance in a range of areas and designing a specific information page for services which host pornography;[435] and
- developing a set of interactive compliance tools to make the requirements more accessible and attainable and produced materials, including a series of webinars, to help services understand their duties under the Act.

4.88 We recognise that it may take time for service providers to understand the new regime, assess the risks their services pose to users and make the necessary adaptions to their systems and processes. This is likely to particularly be the case for smaller services, those new to regulation, and services within scope of both Part 5 and Part 3 of the Act. We will take these challenges into account when considering whether and when it is appropriate to take enforcement action against non-compliance with the Part 5 duties.

4.89 However, we expect all providers to take a proactive approach to compliance and meet their respective implementation deadlines. Ofcom is opening an age assurance enforcement programme, focusing our attention first on Part 5 services.

4.90 We recognise the risk that users will seek to move to services that do not use age assurance and acknowledge the examples raised by stakeholders from other jurisdictions. We will take

[433] Ofcom, 2024, Investigation into Mintstars ltd compliance with rules to protect children from restricted material
[434] Ofcom, 2024, Implementing the Online Safety Act: progress update.
[435] Ofcom, 2024, available at ofcom.org.uk/adultsonly.

steps to monitor compliance across the adult sector, with services of all sizes, and stand ready to take enforcement action where services do not comply with their duties to use highly effective age assurance to prevent children from encountering pornographic content, both under Part 5, and when they come into force, under Part 3. We will also be engaging in public awareness campaigns to encourage adults to engage with age assurance rather than visit sites that may be less safe.

Next steps

4.91 Part 5 services are required to comply with their duties under the Act, including the requirement to use highly effective age assurance, from 17 January 2025. As such, they must take steps to introduce highly effective age assurance immediately.

4.92 Part 5 providers should refer to the final Part 5 Guidance, as well as this Section 3 of this statement, to understand how they can meet all the requirements of the Act relating to the scope of Part 5.

5. Children's access assessments

In this section, we set out our consideration of stakeholder responses that we received on our proposed approach to children's access assessments and our draft Children's Access Assessments Guidance, together with reasons for reaching our decisions.

A children's access assessment is a process that all providers of Part 3 services in scope of the Act must carry out to determine whether a service, or part of a service, is likely to be accessed by children. Ofcom is required to produce guidance to assist service providers in complying with their children's access assessments duties.

Broadly, we have decided to confirm the approach we proposed in our May 2024 Consultation in relation to the areas where we have exercised our policy discretion, as follows:

- Service providers should only conclude that it is not possible for children to access a service (or part of a service) where they are using highly effective age assurance to control access to the service.
- What constitutes a significant number of children for the purposes of a children's access assessment depends on the nature and context of each service.
- We have set out in the Children's Access Assessments Guidance a list of factors that services should take into account when carrying out their assessment of whether the child user condition is met. Services must record the outcome of children's access assessments. The process should be a straightforward exercise for most providers. Services that conclude that they are not likely to be accessed by children should be prepared to demonstrate this with a detailed evidence-based assessment.

Providers may already have assessed whether they are likely to be accessed by children as set out in the ICO's Children's code for the purposes of complying with data protection regulation, and may be able to draw on similar evidence and analysis for carrying out both assessments.

Introduction

5.1 A children's access assessment is a process for establishing whether a service, or part of a service,[436] is "likely to be accessed by children".[437] We anticipate that most Part 3 services that are not using highly effective age assurance are likely to be accessed by children within

[436] Unless otherwise indicated, references in this section to "service" should be read as "service or part of a service".
[437] Section 37 of the Act.

the meaning of the Act.[438] Services likely to be accessed by children must comply with the children's risk assessment duties[439] and the children's safety duties.[440]

5.2 Ofcom has a duty to produce guidance to assist service providers in complying with the duties relating to children's access assessments.[441] This section explains our approach to the Children's Access Assessments Guidance.

5.3 Children's access assessments have two stages:[442]

- **Stage 1:** The service provider must determine whether it is possible for children to access the service or a part of it.[443] A provider is only entitled to conclude that it is not possible for children to access a service if it is using age assurance with the result that children are not normally able to access it.[444]
- **Stage 2**: If it is possible for children to access a service, or a part of a service, the service provider must then determine whether the "child user condition" is met.[445]

5.4 Children's access assessments must be suitable and sufficient.[446] Services that do not have highly effective age assurance in place must carry out stages 1 and 2 of the child access assessment. Services that have highly effective age assurance in place and reach the conclusion that therefore it is not possible for children to access the service need only complete stage 1, then record the outcome of their assessment. If a provider concludes that the child user condition is not met (stage 2), in order to have carried out a suitable and sufficient assessment they must make a written record of the steps they have taken to reach their conclusion, supported by evidence.

5.5 Where it is possible for children to access a service (or part of it), the child user condition is met if:

- there is a significant number of children who are users of the service or that part of it; **and/or**
- the service, or that part of it, is of a kind likely to attract a significant number of users who are children.[447]

5.6 The two parts of the child user condition are not cumulative. If either (or both) of the criteria are met, the service is considered as "likely to be accessed by children" and needs to comply with the duties under sections 11 and 12 of the Act (if the service is a U2U service) or sections 28 and 29 of the Act (if the service is a search service or for combined services in

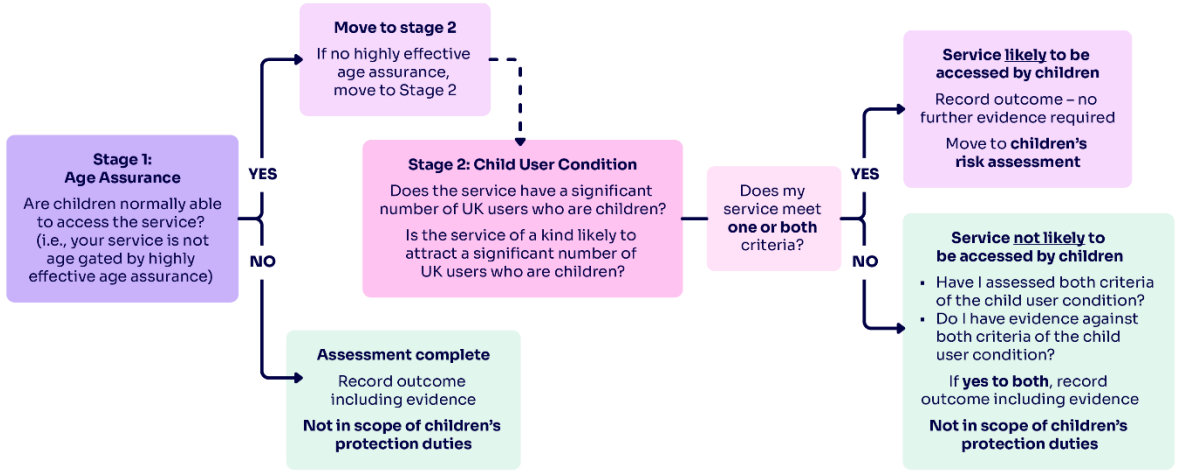
[438] Section 37 of the Act.
[439] Sections 11 (U2U services) and 28 (search services) of the Act.
[440] Sections 12 (U2U services) and 29 (search services) of the Act.
[441] Section 52(3)(b) of the Act.
[442] Whether both stages need to be completed depends on the outcome of stage 1 for a service provider. We provide further guidance on this in Sections 2 and 3 of the Children's Access Assessments Guidance.
[443] Section 35(1)(a) of the Act.
[444] Section 35(2) of the Act. As we note in the Children's Access Assessments Guidance, whether a service is likely to be accessed by children is assessed differently under data protection law for the purposes of the ICO's Children's code and services should consult the ICO's guidance where appropriate.
[445] Section 35(1)(b) of the Act.
[446] Section 36(6) of the Act.
[447] Section 35(3) of the Act.

relation to the search engine of each such service).[448] This means they must carry out a children's risk assessment, as discussed at Section 12 of our May 2024 Consultation on Protecting Children from Harms Online ("May 2024 Consultation"), and use or adopt appropriate measures to comply with the safety duties protecting children, as discussed at Section 14 of our May 2024 Consultation.

5.7 Where a service provider fails to complete a children's access assessment, the service will be treated as likely to be accessed by children.

5.8 The children's access assessments process is shown in Figure 5.1 below.

Figure 5.1: Children's access assessments process



Source: Ofcom

5.9 Our Children's Access Assessments Guidance seeks to assist service providers in complying with their duties in relation to children's access assessments by setting out a clear process and recommended factors and evidence to consider at each stage. The process will be straightforward for most providers. Where providers conclude that their service is likely to be accessed by children, we will not expect them to record in detail the evidence supporting this conclusion, enabling them to move on to the children's risk assessment and use their time and resources efficiently. Where providers conclude that their service is not likely to be accessed by children, we will expect them to record the evidence supporting their conclusion.

Our proposals

5.10 In our May 2024 Consultation, we set out our proposed approach to parts of the draft Children's Access Assessments Guidance where we exercised some degree of discretion, and invited stakeholders' feedback on our proposed approach on these particular areas:

[448] A combined service is a regulated U2U service that includes a public search engine, as defined at section 4(7) of the Act.

- **Age assurance for children's access assessments:** we proposed that where providers conclude that it is not possible for children to access a service, or a part of it, because they are using age assurance, that age assurance should be "highly effective".
- **Our approach to the child user condition:** we provided a non-exhaustive list of indicative factors to consider when assessing both criteria of the child user condition. We proposed that providers take a holistic approach, considering a range of factors to determine which criterion of the child user condition to begin with.
- **What constitutes a "significant number" of children:** we proposed that a relatively small number or percentage of children could be a significant number depending on the context.
- **How service providers can assess whether they are "of a kind likely to attract a significant number of children":** we recommended that providers consider the factors provided in the Children's Access Assessments Guidance, and any other relevant factors, to build an understanding of whether their service is likely to attract a significant number of children.

Our approach to children's access assessments

5.11 Some respondents made general comments or gave feedback on our overall approach to children's access assessments. We have considered these responses, summarised them below, and responded in a number of areas in the sub-section "Our decision" below.

Summary of responses

5.12 Two respondents broadly agreed with our proposed approach to children's access assessments.[449] 5Rights agreed with our proposed approach "in casting the net widely when determining which services are in scope of the child safety duties."[450]

5.13 Mid Size Platform Group suggested that children's access assessments should contain some consideration of the risk that a service poses to children, to allow low risk services to rule themselves out from the outset.[451] Open Rights Group focused on "non or semi-commercial services not located in the UK" and suggested that "Ofcom's advice should make it clear that such services are not in scope".[452]

5.14 Some stakeholders commented on the three-month timeline for completing children's access assessments. Pinterest asked Ofcom to give consideration to extending the implementation period for children's access assessments in response to feedback from service providers.[453] Other respondents thought the three-month timeline was too long.[454]

[449] CELCIS response to our May 2024 Consultation, p.2; Meta response to the May 2024 Consultation, p.5.
[450] 5Rights Foundation response to May 2024 Consultation, p.4.
[451] Mid Size Platform Group response to our May 2024 Consultation, p.2.
[452] Open Rights Group response to our May 2024 Consultation, p.2.
[453] Pinterest response to our May 2024 Consultation, p.6.
[454] Barnardo's response to our May 2024 Consultation, p.5; CARE response to our May 2024 Consultation, p.2;

Online Travel UK asked whether children's access assessments could be recorded as part of the illegal content risk assessment process.[455]

5.15 Some respondents asked how we would check compliance with the children's access assessments duties and/or enforce against non-compliant services.[456] The Association of Police and Crime Commissioners asked whether Ofcom would be reviewing the assessments of services that determined the number of children not to be significant, and correcting any assumptions made that we disagreed with.[457] NSPCC called for further information "about how Ofcom will identify and prioritise scrutinising the assessments of borderline services who have determined that they are not likely to be accessed by children, new services which grow rapidly, and those operating in flagrant breach of the regulation."[458]

Our decision

5.16 Having carefully considered stakeholder responses to our consultation, we have decided to adopt the approach to children's access assessments that we proposed in our May 2024 Consultation. We have made some minor changes to the Children's Access Assessments Guidance in response to stakeholder comments, which we explain at the end of the sub-section *Assessing whether the child user condition is met* (from paragraphs 5.85).

5.17 Providers are required by the Act to carry out children's access assessments for all Part 3 services. We do not have discretion to waive the children's access assessments duties for Part 3 services located outside the UK, or for non-or semi-commercial services, as suggested by Open Rights Group. Nor do we have discretion to waive the requirements for certain types of services that may pose a low risk to children, as one respondent suggested.

5.18 The timing for carrying out the first children's access assessment depends on when a service comes within the scope of Part 3 of the Act, as set out in Section 2 of the Children's Access Assessments Guidance. In response to Pinterest, given that in general we expect that for most services this should be a straightforward exercise, we consider that services should need no more than three months to complete children's access assessments. In response to stakeholders who felt the period for completing children's access assessments was too long, we do not have discretion to require services to complete children's access assessments in less than three months.[459]

5.19 In response to the stakeholder query about whether children's access assessments could be recorded as part of the illegal content risk assessment process, we remind providers that they are required to complete illegal content risk assessments for **all** Part 3 services by 16 March 2025.[460] They may carry out and record the results of their children's access

---

CEASE response to our May 2024 Consultation, pp.2-4; Christian Institute response to our May 2024 Consultation, p.2.

[455] Online Travel UK response to our May 2024 Consultation, p.6.

[456] Association of Police and Crime Commissioners response to our May 2024 Consultation, p.4; Health Professionals for Safer Screens response to our May 2024 Consultation, p.3; Yoti response to our May 2024 Consultation, p.6.

[457] Association of Police and Crime Commissioners response to our May 2024 Consultation, p.4.

[458] NSPCC response to our May 2024 Consultation, p.6.

[459] Part 1 of Schedule 3 to the Act.

[460] See Ofcom, Risk Assessment Guidance and Risk Profiles.

assessments at the same time, but will be required to carry out separate children's risk assessments in the event that they determine a service is likely to be accessed by children, within three months of the publication of our final Children's Risk Assessment Guidance. We will publish our final Children's Risk Assessment Guidance in April alongside our Protecting Children from Harms Online Statement.

5.20 In response to stakeholders who asked about our approach to compliance and enforcement, as discussed in Section 2 of the Children's Access Assessments Guidance, if we suspect that a service has failed to carry out a suitable and sufficient children's access assessment properly or at all, then we may consider taking enforcement action in line with our OS Enforcement Guidance.[461] We have the power to impose a financial penalty of up to 10% of qualifying worldwide revenue or £18 million (whichever is the greater), and can also require remedial action to be taken. Remedial action may include Ofcom requiring the service to comply with the children's risk assessment duties and the children's safety duties.[462]

Stage 1: Age assurance for children's access assessments

Background

5.21 The first stage of a children's access assessment is to determine whether it is possible for children to access the service or a part of it. Under the Act, a provider is only entitled to conclude that it is not possible for children to access a service, or a part of it, if it is using age assurance with the result that children are not normally able to access it.[463] Where a service provider concludes that this requirement is met, this concludes the children's access assessment and the service is not in scope of the children's risk assessment and safety duties.

5.22 The Act does not specify the type of age assurance providers should use in this context. Ofcom has discretion on the approach that we deem to be most appropriate for the purpose of children's access assessments.

Our proposals

5.23 As set out from paragraph 4.14 of our May 2024 Consultation and in Section 3 of the draft Children's Access Assessments Guidance, we proposed that providers should only conclude that it is not possible for children to access a service (or the relevant part of it) if:

- they have implemented age assurance which is highly effective at determining whether or not a particular user is a child; **and**

[461] See Ofcom, Protecting People from illegal harms online: online safety enforcement guidance. Published 16 December 2024.
[462] Section 135 of the Act.
[463] Section 35(2) of the Act.

- they have access control measures that prevent users from being able to normally access the service, or the relevant part of it, except for users identified as adults via their age assurance process.[464]

5.24 To help services to understand what constitutes highly effective age assurance, we referred services to our draft Part 3 HEAA Guidance which we published as Annex 10 of our May 2024 Consultation.[465] We proposed that the same criteria and principles would apply when assessing age assurance in the context of carrying out children's access assessments. We advised services that they would need to consider the Part 3 HEAA Guidance should they wish to carry out an in-depth assessment of whether a particular form of age assurance is highly effective for the purpose of this first stage of the children's access assessment.

Summary of responses

5.25 A range of respondents expressed broad support for our proposal that service providers should only conclude that children are not normally able to access a service where they are using highly effective age assurance.[466]

5.26 Northeastern University London said that there may be other ways of providing assurance that children are not normally able to access a service without relying on highly effective age assurance.[467] Inkbunny noted that search engines filter pages with Restricted to Adults (RTA) tags[468] or other adult rating tags, and said this should be considered when determining whether a service is likely to be accessed by children.[469] The Online Dating and Discovery Association argued that a risk-based approach would be more proportionate.[470]

[464] We use the term "access controls" to describe a technical mechanism(s) which prevents users who have not been age assured, or having been age assured, did not meet the requirements of the age assurance process, from accessing a service (or part of it) or certain content.
[465] See Section 3: Ofcom's approach to highly effective age assurance.
[466] Age Check Certification Scheme response to our May 2024 Consultation, p.2; Bandio response to our May 2024 Consultation, p.2; Barnardo's response to our May 2024 Consultation, p.4; Canadian Centre for Child Protection response to our May 2024 Consultation, p.2; CEASE response to our May 2024 Consultation, p.2; CELCIS response to our May 2024 Consultation, p.2; Children's Commissioner for England response to our May 2024 Consultation, p.3; Christian Institute response to our May 2024 Consultation, p.2; Commissioner Designate for Victims of Crime Northern Ireland response to our May 2024 Consultation, p.3; Dean, J. response to our May 2024 Consultation, p.2; Derbyshire OPCC Police response to our May 2024 Consultation, p.2; East Riding Safeguarding Children Partnership response to our May 2024 Consultation, p.1; Institution of Engineering and Technology response to our May 2024 Consultation, p.2; Kooth Digital Health response to our May 2024 Consultation, p.2; The LEGO Group response to our May 2024 Consultation, p.1; Mobile Games Intelligence Forum response to our May 2024 Consultation, p.1; National Crime Agency response to our May 2024 Consultation, p.2; Nexus response to our May 2024 Consultation, p.2; Smartphone Free Childhood response to our May 2024 Consultation, p.2; Ukie response to our May 2024 Consultation, p.4; Veridas response to our May 2024 Consultation, p.2.
[467] Northeastern University response to our May 2024 Consultation, p.7.
[468] Restricted to Adults (RTA) tags provide a means for services to indicate that their content is not appropriate for children so that the service is made inaccessible for users with parental control filters applied.
[469] Inkbunny response to our May 2024 Consultation, p.2.
[470] Online Dating and Discovery Association response to our May 2024 Consultation p.2.

5.27 One respondent suggested that services offering gambling, alcohol, tobacco or weapons should be required to have systems in place to exclude children.[471]

5.28 Other respondents disagreed with one or more aspects of our proposals in relation to age assurance for children's access assessments.[472]

5.29 Some suggested that services might choose to use highly effective age assurance to block children altogether rather than creating child safe experiences.[473] Integrity Institute argued that "age assurance overall provides a poor grounding and foundation for child safety."[474]

5.30 Two respondents expressed concern that children may still be able to access services where highly effective age assurance is in place.[475] Yoti felt that Ofcom should be clearer about how services should quantify 'normally' in the context of children 'not normally' being able to access a service and suggested Ofcom's guidance should take into account children's ability to circumvent age assurance methods, for example through the use of VPNs.[476] Yoti also proposed Ofcom carry out periodic independent reviews of the various age assurance solutions employed by providers in scope of the regime.[477]

Our decision

5.31 The Act makes clear that a provider is only entitled to conclude that it is not possible for children to access a service, or a part of it, if age verification or age estimation is used on the service with the result that children are not normally able to access the service or that part of it.[478] It is not therefore open to us to state that methods other than use of age assurance may secure the result that children cannot normally access the service, or to adopt a risk-based approach, as some stakeholders suggested.

5.32 Having carefully considered stakeholder responses to the consultation, we have decided to confirm the approach we proposed in our May 2024 Consultation, which is that providers should only conclude that it is not possible for children to access the service where they are using highly effective age assurance to control access to the service. The Children's Access Assessments Guidance should therefore be read in conjunction with the Part 3 HEAA Guidance, which we discuss in Section 3 of this statement.

---

[471] Carr, J response to our May 2024 Consultation, p.2.
[472] Big Brother Watch response to May 2024 Consultation, pp.2-3; Free Dating Limited response to our May 2024 Consultation, p.2; Global Network Initiative response to our May 2024 Consultation, pp.4-5; Northeastern University London response to our May 2024 Consultation, pp.8-9; Online Dating and Discovery Association response to our May 2024 Consultation, pp.2-4; Parenting Focus response to our May 2024 Consultation, pp.2-5; Elliott, R. response to our May 2024 Consultation, p.2; techUK response to our May 2024 Consultation, p.2.
[473] Big Brother Watch response to our May 2024 Consultation, p.3; Global Network Initiative response to our May 2024 Consultation, p.4; Samaritans response to our May 2024 Consultation, p.4.
[474] Integrity Institute response to our May 2024 Consultation, p.2.
[475] Association of Police and Crime Commissioners response to our May 2024 Consultation, p.3; Health Professionals for Safer Screens response to our May 2024 Consultation, pp.2-3.
[476] Yoti response to our May 2024 Consultation, p.5.
[477] Yoti response to our May 2024 Consultation, p.7.
[478] Section 35(2) of the Act.

5.33 Having considered responses questioning the appropriateness and feasibility of highly effective age assurance, we remain of the view that highly effective age assurance is the most appropriate way of ensuring that children are not normally able to access the service, pursuant to the requirement of the Act. As we said in our May 2024 Consultation, this approach is consistent with Ofcom's duty to have regard to the need for a higher level of protection for children than for adults.[479] In addition, as noted in our consultation, our approach provides consistency for U2U services across the range of duties they may be required to meet.

5.34 We considered other approaches to age assurance for children's access assessments, for example based on a lower standard of effectiveness, or accepting any form of age assurance as being acceptable for this purpose. We took the view that such alternative approaches would potentially leave children vulnerable to harm if ineffective age assurance is implemented by a provider, with the result that the service provider would wrongly conclude it was not in scope of the children's risk assessment and safety duties and would not take appropriate steps to keep children safe from the risk on that service even though they would be able to access the service.

5.35 As discussed in Section 3 of this statement, services that choose to use methods that are not listed in the Part 3 HEAA Guidance should therefore consider if they can be implemented in a way that meets the criteria for highly effective age assurance and should only adopt them if they can implement in a way that does meet the criteria.

5.36 We do not have discretion to require that particular types of Part 3 service, for example those hosting or making available content that offers offering gambling, alcohol, tobacco or weapons, should be required to exclude children as one stakeholder suggested. There may be other legal requirements outside the scope of the Act which such services would be expected to implement so as to prevent children from accessing age-controlled products and services.

5.37 The children's access assessment duties do not **require** use of highly effective age assurance and nor does our guidance recommend that providers should seek to adopt it rather than creating a child-safe experience for children on their service as required by the children's safety duties. We acknowledge that – as noted by some respondents – some providers may decide to implement highly effective age assurance rather than creating a child-safe experience, particularly services that are not intended to be accessed by children. However, this is a commercial decision for those organisations.

5.38 We acknowledge that highly effective age assurance will not always be effective in preventing all children from accessing the service as some children may be able to circumvent it. We have addressed circumvention in Section 3 of this statement, in the sub-section on robustness (from paragraph 3.138).

[479] As set out in section 3(4A)(b) of the 2003 Act, as inserted by the Act.

Stage 2: The child user condition

Background

5.39 Where it is possible for children to access a service, or part of the service, the child user condition in the Act is met if:

- "there is a **significant number** of children who are users of the service or of that part of it; **or**
- the service, or that part of it, is of a kind likely to attract a **significant number** of users who are children."[480]

5.40 We have interpreted "or" as "and/or", such that the child user condition is met if **one or both** of the criteria is met. We consider that this is consistent with the intention of the Act.[481] Services can only conclude that the child user condition is not met if they have evidence that demonstrates that neither of the two criteria are met. As we note below and in the guidance, it may be easier for some providers to start with the second criterion. We received a number of stakeholder comments on the concept of "significant number" in the child user condition, including on our proposal not to suggest any numerical threshold over which the number or proportion of children would be considered significant. We set out our proposals, stakeholder responses and our final position on "significant number", before going on to consider our other proposals in relation to assessing whether the child user condition is met.

Significant number

Our proposals

5.41 In our May 2024 Consultation we proposed that what constitutes a "significant number" of children for the purposes of a children's access assessment is likely to depend highly on the context, taking into account a number of factors and characteristics.[482]

5.42 We said that, given the potential for serious harm, even a relatively small absolute number or proportion of children could be significant in terms of the risk of harm to children.[483] We said that we considered the term should be understood as indicating that the number of children on the service is material in the context of the service in question.[484]

5.43 We noted that our proposed approach to "significant number" applied to both criteria of the child user condition.[485]

---

[480] Section 35(3) of the Act.
[481] It would be a perverse outcome if a service concluded that it was not likely to be accessed by children because it had met both criteria, rather than just one. Logically, services of a kind likely to attract children are more likely than other kinds of services to have a significant number of child users.
[482] May 2024 Consultation, paragraph 4.22, referring to 'Likely to be accessed' by children – FAQs, list of factors and case studies. | ICO.
[483] Draft Children's Access Assessments Guidance, paragraphs 4.7-4.8.
[484] Draft Children's Access Assessments Guidance, paragraph 4.9.
[485] May 2024 Consultation, paragraph 4.24.

5.44 We did not propose any numerical threshold for what constitutes "significant". We said there was currently no robust basis for setting numerical thresholds, and that if we were to propose a single numerical threshold, this could lead to services that potentially pose a very serious risk of harm to children concluding that they are not in scope of the children's safety duties.[486]

5.45 We explained that we thought our proposed approach to "significant number of children" was compatible with the ICO's guidance on its Children's code.[487]

Stakeholder responses

5.46 A range of respondents expressed broad support for our proposed approach to "significant number of children".[488]

5.47 Big Brother Watch considered our proposed approach to go against the "ordinary meaning" of the term "significant".[489] Google argued our suggestion that most Part 3 services would be in scope[490] did not "reflect the statutory definition in section 35(4)(a) of the Act, which states that "significant" means "significant in proportion to the total number of United Kingdom users of a service", and would have a disproportionate impact on many services. Google suggested we remove suggestions in the draft guidance that a relatively small absolute number or proportion might be "significant", and instead explicitly recognise that services should make their own determinations on what is significant based on relevant considerations, "including the number of impacted child users".[491] Another respondent said that under our proposed approach any number of children could potentially be considered significant.[492]

5.48 Two respondents suggested that our proposed approach would bring too many services in scope of the children's risk assessment duties and children's safety duties. The Advertising Association said that our proposed approach would "increase the likelihood of many more services being classified as "likely to be accessed by children", even if children are not their primary audience", while Google argued our approach would impose "a disproportionate burden to many services".[493]

---

[486] May 2024 Consultation, paragraphs 4.25-4.27.
[487] May 2024 Consultation, paragraph 4.27.
[488] Association of Police and Crime Commissioners response to our May 2024 Consultation, p.4; Canadian Centre for Child Protection response to our May 2024 Consultation, p.2; CELSIS response to our May 2024 Consultation, p.2; Children's Commissioner for England response to May 2024 Consultation, p.4; Microsoft response to our May 2024 Consultation, p.2; Nexus response to our May 2024 Consultation, pp.2-3; Northern Ireland Commissioner for Children and Young People (NICCY) response to our May 2024 Consultation, p.21; NSPCC response to our May 2024 Consultation, p.3; Welsh Government response to our May 2024 Consultation, p.2.
[489] Big Brother Watch response to our May 2024 Consultation, p.4.
[490] May 2024 Consultation paragraph 4.44.
[491] Google response to our May 2024 Consultation, p.7.
[492] [✂]
[493] Advertising Association response to our May 2024 Consultation, p.3; Google response to our May 2024 Consultation, p.7.

5.49 A range of respondents suggested that we could provide further clarity on what was meant by a significant number of children.[494]

5.50 Three respondents proposed that the determination of whether the number of child users on a particular service is significant should be informed by likelihood of harm to children on that service.[495] However, the Scottish Government found our interpretation of significant number of children unclear, as they interpreted the child user condition as requiring an "in-context numerical assessment, as opposed to any weighing up of risks of potential harm (which follows once the user condition is met)".[496]

5.51 Bandio expressed support for our proposals, but said it would be helpful to provide "case study examples on both ends of the spectrum: where objectively a low number of users are children, but the context risks are high enough for Ofcom to consider the number 'significant'; and the reverse, i.e. a larger number of children but representing very low context risk and the conditions under which Ofcom would not consider this to be significant."[497] Bandio also suggested we provide "examples of context risks that Ofcom would consider so high as to result in any number of child users to be significant".[498]

5.52 Several respondents suggested that Ofcom should align more clearly with the ICO's approach to significant number.[499]

5.53 X said it was important for services to understand how Ofcom interprets a "user", including for the purpose of determining a significant number of children.[500] Ukie argued that calculation of user numbers should be carried out differently for gaming compared to social media due to the differences in user behaviour.[501]

5.54 Some respondents commented on our proposal not to specify numerical thresholds for significant number. Derbyshire Police and an individual respondent suggested a two-criteria approach, whereby a number is considered significant if it meets either of two thresholds, one expressed as an absolute number and one as a percentage.[502] Two respondents suggested that any number greater than zero could be considered a significant number of

---

[494] Association of Police and Crime Commissioners response to our May 2024 Consultation, p.4. Institution of Engineering and Technology response to our May 2024 Consultation, p.3;The LEGO Group response to our May 2024 Consultation, p.1; Mid Size Platform Group response to our May 2024 Consultation, p.4; Online Dating and Discovery Association response our May 2024 Consultation, p.4; Pinterest response to our May 2024 Consultation, p.6; Scottish Government response to our May 2024 Consultation, p.2; techUK response to our May 2024 Consultation, p.2.

[495] [✂]; the Global Network Initiative response to our May 2024 Consultation, p.4; Wikimedia Foundation response to our May 2024 Consultation, pp.4-5.

[496] Scottish Government response to our May 2024 Consultation, p.2.

[497] Bandio response to our May 2024 Consultation, p.3.

[498] Bandio response to our May 2024 Consultation, p.3.

[499] Google response to our May 2024 Consultation, p.7; Online Travel UK response to our May 2024 Consultation, p.5; Yoti response to our May 2024 Consultation, p.4.

[500] X response to our May 2024 Consultation, pp.1-2.

[501] Ukie response to our May 2024 Consultation, p.7.

[502] Derbyshire OPCC response to our May 2024 Consultation, p.3; Dean, J response to our May 2024 Consultation, p.3.

children.[503] 9000 lives suggested that leaving uncertainty about what constitutes a significant number of children leaves flexibility for services that may put children at undue risk.[504] However, Microsoft agreed with our approach, noting that numerical thresholds "may not reflect the context of a unique service".[505]

Our decisions

5.55 Having carefully considered stakeholder responses to our May 2024 Consultation, we remain of the view that what constitutes a significant number of children for the purposes of a children's access assessment is likely to be highly dependent on the nature and context of each service.

5.56 The Act says that "a "significant" number includes a reference to a number which is significant in proportion to the total number of United Kingdom users of a service".[506] In response to Google's comment that significant should be understood as being in proportion to the total number of users, we interpret the Act as meaning that 'significant' could refer to either an absolute number or a proportion of the UK user base.

5.57 We disagree with stakeholders that our approach is inconsistent with the ordinary meaning of "significant". Given the clear intent of the Act to ensure that regulated services are designed and operated in a way that secures a higher standard of protection for children than for adults, we remain of the view that it could not be the intention of Parliament that the concept of a "significant number of children" within the meaning of the Act should require the number in question to be a large or substantial number, either in absolute terms or as a proportion of child users compared to the overall UK user base. Instead, we remain of the view that this term should be interpreted to mean a material number of children, when considering the nature and context of the service.

5.58 Our approach takes into account that even a relatively small absolute number or proportion of children could be significant in terms of the harm that may be experienced by children on services. We do not agree with respondents who argued that our interpretation will lead to services inappropriately being in scope of the children's safety duties. Services that conclude that they have a significant number of children (or are of a kind likely to attract a significant number of children) may still conclude that they are low risk to children when they undertake their children's risk assessment, limiting the range of measures that they need to have in place to address those risks. We therefore agree with the Scottish Government that consideration of the risk of potential harm to children should take place *after* a service provider has determined that a service is likely to be accessed by children – this is the role of children's risk assessments.

5.59 In response to stakeholders who asked for further clarity on what was meant by a significant number of children, we have set out above that the meaning of significant will depend on the nature and context of a service, and we have provided guidance to this end for services to consider with regards to their service or part of their service. As we noted in our May

[503] Association of Police and Crime Commissioners response to our May 2024 Consultation, p.4; Health Professionals for Safer Screens response to our May 2024 Consultation, p.2.
[504] 9000 Lives response to our May 2024 Consultation, p.1.
[505] Microsoft response to our May 2024 Consultation, p.2.
[506] Section 35(4)(a) of the Act.

2024 Consultation, our guidance on significant number of children applies to both criteria of the child user condition.

5.60 Our approach offers service providers the flexibility to consider a variety of factors (as discussed further below) that may suggest that the child user condition is met. We consider that this approach strikes the right balance, providing some clarification as to the kinds of factors we expect service providers to have regard to in carrying out children's access assessments, while not being overly prescriptive. We have included some illustrative case studies in the Children's Access Assessments Guidance to assist service providers in considering what factors may be relevant for them. We have not included any additional case studies (as requested by stakeholders) as we think they already cover a reasonable range of different factors. However, in response to stakeholder feedback we have incorporated in the case studies some additional factors and considerations which should support service providers in assessing what factors may be relevant in the context of their service.

5.61 We do not suggest that providers should take any particular steps to gather evidence on how users (including children) react to content or the design features of a service. As part of their holistic assessment of the service, providers can consider any data on the number of users if available (and reliable), but we do not recommend collecting any specific or new information. Where services already collect user data, they must ensure they process any personal data in a manner compliant with data protection and privacy laws. The relationship between children's access assessments and data protection and privacy law is set out within our impact assessment at Annex 2.

5.62 In response to stakeholders who commented that our approach to "significant number" was inconsistent with that of the ICO, we remain of the view set out in our May 2024 Consultation that our approach is compatible with the ICO's guidance on its Children's code which, similarly, does not offer a numerical threshold for "significant" in assessing whether a service is "likely to be accessed by children", and also encourages providers to consider a range of relevant factors in their assessments.

5.63 In response to comments about the definition of a user and calculation of user numbers, we note that the term "user" is defined in the Act.[507] It does not matter whether a user is registered to use a service.[508] For U2U services, it is not necessary for users to post or upload content – merely viewing (or otherwise encountering) U2U content on a service counts as actively using that service.[509]

5.64 As proposed in our May 2024 Consultation, our Children's Access Assessments Guidance does not suggest any numerical threshold for what a "significant number of children" may be.

5.65 The Act does not make provision for us to set any legally binding numerical thresholds in the context of the child user condition. We considered whether suggesting an indicative threshold would assist services in complying with their duties in relation to children's access

[507] Section 227 of the Act.
[508] Section 227(2) of the Act.
[509] Section 3(2)(a) of the Act.

assessments. In practice, however, a large number and variety of services are in scope of Part 3, and we lack robust evidence (particularly about smaller services) that could give us the basis to specify any value. We note that consultation respondents did not suggest the level of UK child users at which a threshold could be set, or suggest any data sources or methodologies that could be used as a potential basis for such a threshold.

5.66 In the absence of robust evidence or data sources, there is a risk that any value we include could create a material risk of unintended consequences affecting a large number of services and users. Setting a threshold too high could lead to many services that potentially pose a serious risk of harm to a relatively small number of children concluding wrongly that they are not in scope of the children's safety duties. Setting the threshold too low could mean that many services that do not attract material numbers of children in the UK and pose a negligible risk of harm to children are brought into scope of the children's safety duties in a way which could be disproportionate.

5.67 The benefit of providing thresholds would also be limited for providers that lack precise and robust data on the age of users to determine whether they are above or below any numerical threshold. As we implement the regime, we will continue to build our evidence base and will consider if it becomes possible and appropriate to provide further guidance on indicative thresholds.

5.68 We do not agree with stakeholders' suggestions that we should define a "significant number of children" as any number greater than zero. The purpose of children's access assessments is to identify services likely to be accessed by children, rather than any service that could be used by a single child.

Assessing whether the child user condition is met

Our proposals

5.69 In our May 2024 Consultation we said that it should be straightforward for a provider to determine whether a service is likely to meet the child user condition. In our draft guidance, we proposed a relatively broad list of factors that could mean a service meets one or both criteria of the child user condition,[510] based on our evidence of children's online habits.[511] We noted that all the factors were relevant for the second criterion of the child user condition and that some of them might also be relevant for the first.[512]

5.70 We recommended that services take a holistic approach to considering whether the child user condition is met. This is because we recognised that it may be challenging for most service providers that are not using highly effective age assurance to accurately determine if their users are adults or children for the purposes of carrying out a quantitative assessment (as indicated by the first criterion of the test).[513] We noted that focusing on the second criterion first may for many services be the more expedient approach to the assessment.[514]

[510] Draft Children's Access Assessments Guidance, p.19 Table 7.
[511] May 2024 Consultation, Section 5.
[512] May 2024 Consultation, paragraph 4.33.
[513] May 2024 Consultation, paragraph 4.38.
[514] May 2024 Consultation, paragraph 4.39.

5.71 We said that there were some types of evidence that were not sufficiently accurate or reliable for confirming that a user is not a child, or might not accurately capture the number of users on a service who are children.[515]

5.72 We said we thought that, based on the available evidence, the child user condition is likely to be met for most Part 3 services that can be accessed by children.[516]

Stakeholder responses

Approach

5.73 The Association of Police and Crime Commissioners expressed support for our suggestion that in most cases it will be appropriate for services to consider whether their service of a kind likely to attract children first when reviewing whether the child user condition is met.[517]

5.74 One respondent argued that age assurance should not be the only way that providers can conclude that it is not possible for children to access their service.[518] Two respondents called for further guidance on how services can demonstrate that they do not have a significant number of child users.[519] Online Travel UK said that the Children's Access Assessments Guidance should explicitly recognise that low-risk services which do not deploy highly effective age assurance can still conclude the child user condition is not met.[520] Northeastern University London suggested that Ofcom could revise the process "such that services which are certain they do not appeal to children could forgo age assurance".[521] Skyscanner suggested that Ofcom provide additional ways for services not using highly effective age assurance to evidence that children are not likely to access their services.[522]

5.75 Several respondents suggest that more should be done to make it clear that children access services that are not specifically aimed at them.[523] NSPCC suggested we should make it clearer that children engage with content due to interest and enjoyment, but also due to peer pressure and curiosity, including content that may be harmful.[524] Online Travel UK said that "whether or not a service expressly bans under 18s in its terms and conditions should not be determinative of whether that service is considered to be accessed by a significant number of child users".[525]

5.76 Mega argued that our proposed approach is not practical for "utility services" that are end-to-end encrypted. They said that in their view "if a service is not designed/intended to

[515] May 2024 Consultation, paragraphs 4.41-4.42.
[516] May 2024 Consultation, paragraph 4.44.
[517] Association of Police and Crime Commissioners response to our May 2024 Consultation, p.4.
[518] Mid Size Platform Group response to our May 2024 Consultation, pp.2-3.
[519] [✂]; Wikimedia Foundation response to our May 2024 Consultation, p.5.
[520] Online Travel UK response to our May 2024 Consultation, p.4.
[521] Northeastern University London response to our May 2024 Consultation, p.8.
[522] Skyscanner response to our May 2024 Consultation, p.2.
[523] Association of Police & Crime Commissioners response to our May 2024 Consultation, p.4; Barnardo's response to our May 2024 Consultation, p.4; Children's Commissioner for England response to our May 2024 Consultation, pp.4-5; Commissioner Designate for Victims of Crime Northern Ireland response to our May 2024 Consultation, p.3; Parenting Focus response to May 2024 Consultation, p.3.
[524] NSPCC response to our May 2024 Consultation, p.4.
[525] Online Travel UK response to our May 2024 Consultation, p.4.

appeal to children, does not target children, and has no reason to believe it has any significant number of children access its site(s), that should be sufficient to dispose of the child user condition."[526]

Factors

5.77 Some respondents expressed support for the indicative list of factors in our draft guidance that we suggested services consider when assessing whether the child user condition is met.[527] The ICO said that the factors listed in the draft guidance are broadly the same as those outlined their guidance on the ICO's Children's code and suggested that this should help services to be efficient when completing the assessments across both of our regimes.[528] 5Rights welcomed the alignment of our proposed approach with that of the ICO.[529]Some respondents suggested additional factors to be considered when assessing if the child user condition is met, or suggested ways that the guidance on factors could be clarified.[530] Yoti suggested we include examples of advertising that are appealing to children, including VPN advertising.[531] Parenting Focus suggested that when considering a service's design, we should include visual elements, gamification, interactive features and overall user experience.[532] Barnardo's suggested that we should change our case studies "to be clear that services should not just focus on the content and target audience of their service when assessing if a child is likely to access it, and instead include a focus on functionalities, as is set out in the guidance."[533]

5.78 The Advertising Association said that "the inclusion of factors related to advertising and commercial strategies in determining whether a service is likely to be accessed by children could have implications for advertising-supported services and business models", and expressed concerns that, if a service is deemed likely to be accessed by children, "advertisers and agencies may need to adjust their advertising practices to comply with stricter regulations around advertising to children".[534]

5.79 Smartphone Free Childhood requested examples of services where children form part of a service's commercial strategy.[535]

5.80 Some respondents suggested that the list of factors that we suggested services consider when assessing whether the child user condition was met was too broad and/or

[526] Mega Limited response to our May 2024 Consultation, pp.4-5.
[527] Age Check Certification Scheme response to our May 2024 Consultation, p.13; CELCIS response to our May 2024 Consultation, p.2; Derbyshire OPCC response to our May 2024 Consultation, p.3; Scottish Government response to our May 2024 Consultation, p.3.
[528] ICO, 2024, The Information Commissioner's response to Ofcom's consultation on protecting children from harms online, p.18. [accessed 9 January 2025]
[529] 5Rights Foundation response to May 2024 Consultation, p.4.
[530] Association of Police and Crime Commissioners response to our May 2024 Consultation, p.4; Barnardo's response to our May 2024 Consultation, p.5; NSPCC response our May 2024 Consultation, p.4.
[531] Yoti response to our May 2024 Consultation, p.9.
[532] Parenting Focus response to our May 2024 Consultation, p.3.
[533] Barnardo's response to our May 2024 Consultation, p.5.
[534] Advertising Association response to our May 2024 Consultation, pp.3-4.
[535]Smartphone Free Childhood response to our May 2024 Consultation, p.2.

subjective.[536] In contrast, the National Crime Agency (NCA) argued that we should consider taking a broader approach, adopting the presumption that "all four factors are in place and the company has to justify why it is not the case".[537]

5.81 Inkbunny and Mid Size Platform Group raised the concern that services that do not uniquely appeal to children may be assumed to cater for children based on how their branding or the design of the service is perceived.[538]

Evidence

5.82 Dr Karen Middleton, University of Portsmouth and Conscious Advertising Network highlighted the need to consider children accessing services via apps connected to a household television when considering if a service has a significant number of child users.[539]

5.83 Yoti welcomed our statement that certain types of evidence are not reliable for confirming that a user is not a child,[540] but suggested the Children's Access Assessments Guidance also make clear that the only data on user age that providers should rely on for children's access assessments is data collected through methods listed as capable of being highly effective in the Part 3 HEAA Guidance.[541] Yoti suggested that we should specify that evidence can only be considered acceptable where it is "independent", "reputable", and from an "external third party source."[542]

5.84 The Christian Institute noted that third sector research could play a significant role in determining the types of sites that are commonly accessed by children.[543]

Our decisions

Approach

5.85 Having carefully considered stakeholder responses to our proposals, we have decided to adopt the approach that we proposed in our May 2024 Consultation and the draft Children's Access Assessments Guidance.

5.86 Our Children's Access Assessments Guidance includes a broad list of factors that could mean a service meets one or both criteria of the child user condition. The intention behind the list of factors is to help providers make an informed decision by suggesting sources of evidence they could consider in the context of a service. It is intended to be non-exhaustive and services should not take the list of factors and examples as a tick-box exercise, whereby the child user condition is or is not met based on the number of examples of content that are present, or factors satisfied. We intentionally selected a broad range of factors because our

[536] Mid Size Platform Group response to our May 2024 Consultation, p.4; xHamster response to our May 2024 Consultation, p.6; Yoti response to May 2024 Consultation, p.4.
[537] National Crime Agency (NCA) response to our May 2024 Consultation, p.2.
[538] Inkbunny response to our May 2024 Consultation, p.2; Mid Size Platform Group response to our May 2024 Consultation, p.4.
[539] Dr Karen Middleton, University of Portsmouth and Conscious Advertising Network response to our May 2024 Consultation, p.2.
[540] May 2024 Consultation, paragraph 4.41.
[541] Yoti response to our May 2024 Consultation, p.7.
[542] Yoti response to our May 2024 Consultation, p.6.
[543] Christian Institute response to our May 2024 Consultation, p.2.

evidence suggests that children are attracted by a broad range of online services offering different types of content and features. This list draws on our evidence of children's online habits, which we have updated and reproduced at Annex 3 of this statement.[544]

5.87 Given the breadth of children's online experiences and the range of types of services regulated under Part 3, it would not be feasible for Ofcom to identify a comprehensive list of all relevant factors in the guidance. There may be other sources of evidence that may also help a provider build an understanding of whether their service is likely to be accessed by children. We would not want services that are of a kind likely to attract children to rule themselves out of scope of the children's safety duties because they do not consider that the factors we have listed apply to them.

5.88 As noted in our May 2024 Consultation, we considered an alternative approach of setting out a narrower, more definitive list of criteria. We remain of the view that it would not be sufficiently flexible to apply to the wide range of services in scope of the Act, increasing the likelihood that potentially risky services would rule themselves out of scope of the children's risk assessment and children's safety duties.

5.89 Our approach is similar to that adopted by other agencies. The ICO's guidance on its Children's code includes a list of examples of factors for providers to consider, which includes "the types of content, design features and activities which are appealing to children". In addition to the ICO's guidance, the Irish Commissioner's Fundamentals for a Child-Oriented approach to Data-Processing, California Age-Appropriate Design Code Act and Dutch Code for Children's Rights also include some references to content types.[545]

5.90 It is up to service providers to review our guidance and complete a suitable and sufficient assessment. As our Children's Access Assessments Guidance states, services should consider both criteria of the child user condition and take a holistic view, based on the available evidence, on whether their service is of a kind that is likely to attract children. This does not necessarily require a quantitative assessment based on evidence about user numbers.

5.91 We do not consider that any single factor in the list would always necessarily indicate that a service is of a kind likely to attract a significant number of children. If a service allows a wide range of types of content, this logically means that the service is more likely to have some type of content that appeals to children. If a service only has a narrow range of content, the service provider should then consider, based on the evidence, whether this content is likely to appeal to children. In response to comments from stakeholders who mentioned content types or functionalities not aimed at children, we reiterate that children may be interested in services not aimed primarily (or indeed at all) at them; for example, evidence suggests that children are attracted to dating and pornography services (see paragraph A3.7).

5.92 To stakeholders who requested further clarity on how services can demonstrate that the child user condition is not met, including where they are not using highly effective age

[544] May 2024 Consultation, Section 5.
[545] Irish Commissioner, 2021. Fundamentals for a Child-Oriented approach to Data-Processing. [accessed 22 April 2024] California Legislature, 2022. The California Age-Appropriate Design Code Act. [accessed 22 April 2024], Ministry of the Interior and Kingdom Relation, 2021. The Dutch Code for Children's Rights. [accessed 22 April 2024].

assurance, we think that our approach set out in the Children's Access Assessments Guidance is sufficiently clear. We are not expanding our Children's Access Assessments Guidance to include more detail on how to demonstrate that a service does not have a significant number of child users. The case studies in the guidance include examples of services concluding the child user condition is not met. We have explained that some types of information **are not** appropriate for establishing the number of users on a service that are children.[546] We anticipate that most Part 3 services that are not using highly effective age assurance are likely to be accessed by children within the meaning of the Act.

Factors

5.93 Having carefully considered stakeholder comments, we have adopted the approach we proposed at consultation. We have set out in the Children's Access Assessments Guidance a list of factors that services should take into account when carrying out their assessment of whether the child user condition is met, in line with the four categories we proposed:

- whether the service provides benefits for children;
- whether the content on a service appeals to children;
- whether the design of the service appeals to children; and
- whether children form part of a service's commercial strategy.

5.94 We set out the evidence we drew on in formulating the list of factors in Annex 3 to this statement.

5.95 As noted above, all the factors are relevant for consideration of the second criterion of the child user condition (whether the service is "of a kind likely to attract a significant number of children"), and some may also be relevant for consideration of the first (whether a service has a "significant number of children"). For example, as we explain in the Children's Access Assessments Guidance, if children form part of a service's commercial strategy (that is, its revenue streams are linked to attracting children onto a service) it is reasonable to assume that the service has a significant number of children.[547]

5.96 The ICO provides guidance and resources on its website for its Children's Code, including a list of frequently asked questions, a table setting out examples of factors for services to consider, and a number of case studies providing hypothetical examples of services "not aimed at children assessing whether children access their service in reality." They suggest that content likely to attract children could include, for example, "cartoons, animation, music or audio content, incentives for children's participation, digital functionalities such as gamification, presence of children, influencers or celebrities popular with children",[548] overlapping with some of the types we have suggested in our Children's Access Assessments Guidance. In response to our consultation, the ICO commented that the factors in its own non-exhaustive list of factors that could help information society services to decide whether their services are likely to be accessed by children for the purposes of the ICO's Children's code are "broadly the same as those outlined by Ofcom", and agreed with our suggestion that providers may be able to consider evidence that they might already have gathered for

[546] Children's Access Assessments Guidance, paragraph 4.11.
[547] Children's Access Assessments Guidance, paragraphs 4.32-4.37.
[548] ICO, 'Likely to be accessed' by children – FAQs, list of factors and case studies.

the purposes of assessing themselves against the ICO's Children's code or other guidance, which should help services to be efficient when completing their assessments.[549]

5.97 With regards to the Advertising Association's concern about our inclusion of advertising and commercial strategy as a factor in determining whether a service is likely to be accessed by children, we understand that the UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code) sets rules for advertisers on the targeting of online advertising to children. The CAP regime, which is applied by the Advertising Standards Authority, stands separately from the Act and advertising will continue to be regulated primarily through it.

5.98 We have provided case studies at Annex 2 of the Children's Access Assessments Guidance to support services in understanding how the guidance might be applied in practice. These are illustrative examples that are intended to show how service providers might take into account the factors we have suggested may be relevant.

Evidence

5.99 Where service providers carry out a quantitative assessment against the first criterion of the child user condition (where the service has a significant number of users who are children), they should consider evidence from a range of sources, which could include internal sources (complaints and reporting) and independent research (e.g., market research and quantitative evidence from third parties that track child media consumption), and third sector research as suggested by the Christian Institute.[550] The Children's Access Assessments Guidance provides further detail on the types on internal and external sources that may be useful.[551] As the Advertising Association noted, some providers may be able to draw on advertising data. In response to Yoti's comments, evidence does not necessarily need to be independent – we include in the guidance the example of complaints and reporting data.[552] We do not think it is appropriate to include the word reputable, as what constitutes a "reputable" source would be highly subjective.

5.100 As set out in the Children's Access Assessments Guidance, there are some types of evidence that we do not think are sufficiently accurate or reliable for confirming that a user is not a child, and others may not accurately capture all users on a service and, by extension, the number of users who are children.[553] Noting one respondent's comment that children may access apps via TV, providers should consider the different ways that children might access their service to ensure their assessment is accurate.

5.101 In all cases, where service providers conclude that the child user condition is not met, they should be prepared to demonstrate this with a detailed evidence-based assessment to show that they have carried out a suitable and sufficient assessment.

---

[549] ICO response to our May 2024 Consultation, p.18.
[550] Christian Institute response to our May 2024 Consultation, p.2
[551] Children's Access Assessments Guidance, Section 4.
[552] Children's Access Assessments Guidance, paragraph 4.40.
[553] Children's Access Assessments Guidance, paragraphs 4.11-4.12.

Changes to the guidance

5.102 Further to consideration of responses to consultation, we have made the following minor changes to the Children's Access Assessments Guidance to address stakeholder comments:

- Clarifying that "user" is defined in the Act (paragraph 2.10).
- Drafting changes to paragraphs 3.4, 3.9, 4.11 and 5.21, made for consistency with our Part 3 HEAA Guidance.
- Clarifying that if a service allows a wide range of types of content this logically means that the service is more likely to have some type of content that appeals to children (paragraph 4.17).
- Elaborating on how service providers may consider commercial strategy (paragraph 4.34-4.39).
- Noting that some providers may be able to draw on advertising data (paragraph [4.37).
- Editing the case studies in Annex 2 to make it clearer how service providers could consider commercial strategy.
- Editing the 'large dating service' case study in Annex 2 to make it clear that service providers should consider whether the service includes functionalities that are attractive to children.

Record-keeping duties

Our proposals

5.103 In our May 2024 Consultation, in line with the duty in the Act, we proposed that providers must keep a written record of their children's access assessment outcome in a format that is easily understandable.[554] We provided a template in Annex 1 of the draft guidance to support providers in meeting their record-keeping duties. Service providers may decide to record the outcome in a different format, as long as a written record is kept in a format that is easily understandable.

5.104 We explained that where providers conclude that the child user condition is not met, they should be prepared to demonstrate this with a detailed evidence-based assessment to show that they have carried out a suitable and sufficient assessment. We said this would need to record the methodology they used and the evidence that they have relied on.

Summary of responses

5.105 Yoti proposed that services should be required to publish the outcome of their children's access assessment on their websites.[555] Yoti also considered that record-keeping should be expanded beyond services who consider that the child user condition is not met and should require that all services record whether they conclude that children are normally able to

[554] Section 36(7) of the Act.
[555] Yoti response to our May 2024 Consultation, p.7.

access their service in full or in part, supported by a written record of their evidence base and methodology.[556]

5.106 Google supported our proposals that services need not gather evidence and keep a detailed record of evidence relied upon to support their conclusion where the child user condition is met. Google also supported that the use of our suggested template for record-keeping was optional.[557]

5.107 Health Professionals for Safer Screens were concerned that recording the outcome of a children's access assessment fell to services themselves and that where services conclude that they meet the child user condition, they do not need to record detailed evidence of how they reached this conclusion.[558]

5.108 Microsoft considered our approach to record-keeping for the children's access assessment may place an overemphasis on process and documentation, rather than a focus on identifying existing and new harms, or innovating in safety. They considered that an over-emphasis on formal record-keeping may run counter to a proportionate regulatory regime and that the approach to record-keeping should therefore be flexible.[559]

Our decision

5.109 Having carefully considered stakeholder responses to consultation, we have not made any changes in our approach to the record-keeping duties for children's access assessments. There is no duty in the Act for services to make children's access assessments publicly available, therefore there is no basis for Ofcom to recommend this in the guidance.

5.110 The Act requires that services make and keep a written record of every children's access assessment that they carry out. We have exercised our discretion to recommend that where providers conclude that they meet the child user condition (for either or both criteria), they do not need to record the evidence that supports this conclusion. We consider this approach to be proportionate as it allows services in scope of the child safety duties to then go on to carry out their children's risk assessments, where the Act sets out numerous criteria that must be taken into account. We will therefore be proceeding with our proposed approach to record-keeping for services that meet the child user condition.

Carrying out a new children's access assessment

Our proposals

5.111 Providers of services not treated as likely to be accessed by children must carry out children's access assessments of the service not more than one year apart.[560] As well as services that have concluded they are not likely to be accessed by children, this includes:

[556] Yoti response to our May 2024 Consultation, p.7.
[557] Google response to our May 2024 Consultation, p.7.
[558] Health Professionals for Safer Screens response to our May 2024 Consultation, pp.2-3.
[559] Microsoft response to our May 2024 Consultation, p.2.
[560] Section 36(3) of the Act.

- Services that fail to carry out the first children's access assessment.
- Services that Ofcom has determined should be treated as likely to be accessed by children following an investigation into a failure to comply with any of the children's access assessment duties.

5.112 These two additional scenarios are discussed at paragraphs 2.35-2.37 of the Children's Access Assessments Guidance.

5.113 Providers who have concluded that a service is not likely to be accessed by children are also required to carry out a new assessment under the following specific circumstances that are set out in the Act:

- Before making any significant change to any aspect of the service's design or operation to which such an assessment is relevant.
- In response to evidence about reduced effectiveness of age assurance.
- In response to evidence about a significant increase in the number of children using the service.[561]

5.114 Section 5 of the draft Children's Access Assessment Guidance provided an explanation of each of these circumstances to assist providers assist providers in complying with the requirement to carry out a new children's access assessment in certain circumstances.

Summary of responses

5.115 The Welsh Government agreed that services should carry out a new assessment in response to evidence about a significant increase in the number of children using the service.[562]

5.116 Several respondents welcomed the provision that evidence of the reduced effectiveness of age assurance measures should result in services needing to carry out a children's access assessment.[563] The Centre for Excellence for Children's Care and Protection (CELCIS) emphasised the importance of a proactive cycle of regular review and suggested there could be a greater role for Ofcom in providing scrutiny.[564] Yoti suggested that Ofcom should support providers by periodically reviewing age assurance solutions used by providers, conduct horizon scanning, testing, and publish the results of this work as well as updating its guidance on age assurance accordingly.[565]

5.117 Barnardo's argued that a significant external event, such as the Covid-19 pandemic, should be included as a condition for carrying out a new children's access assessment, because of the impact this could have on children's online behaviour.[566]

5.118 For the examples given of circumstances that amount to a significant change to a service, Meta encouraged the examples listed to be suggested examples of circumstances which may lead to consideration or scoping on whether a new assessment is needed, rather than

[561] Section 36(4) of the Act.
[562] Welsh Government response to our May 2024 Consultation, p.2.
[563] Center for Countering Digital Hate (CCDH) response to our May 2024 Consultation, p.3; Yoti response to our May 2024 Consultation, p.8.
[564] CELCIS response to our May 2024 Consultation, p.7.
[565] Yoti response to our May 2024 Consultation, p.8.
[566] Barnardo's response to our May 2024 Consultation, p.6.

prescriptive criteria that triggers a new assessment.[567] They argue that determining whether a change is significant is highly context dependent and should depend on the potential impact of that proposed change, on the risk to users, and a child's ability to access the service.

5.119 Yoti called for more clarity on what amounts to a significant increase in the number of children using the service.[568]

Our decision

5.120 Having carefully considered stakeholder responses to consultation, we have not made any changes to this section of the Children's Access Assessments Guidance.

5.121 The circumstances that trigger a new assessment are set out in the Act and are not within Ofcom's discretion.[569] A significant external event, such as the one flagged by Barnardo's, might result in an increase in the number of children using a service, which would then mean that the service provider needs to carry out a new assessment.

5.122 Our Children's Access Assessments Guidance is clear that the examples of significant changes to a service that we provide are indicative rather than prescriptive to allow for flexibility and it is for services to assess and determine what circumstances may be relevant. The examples we have provided in the Guidance reflect changes that may result in children accessing a service which they did not previously, or a service becoming more likely to attract children.

5.123 Service providers will need to exercise their own judgement about what a significant increase is in the context of their own service. A significant increase for one service, may not be significant for another and it is up to providers to determine whether there is a significant increase.

Next steps

5.124 All providers of Part 3 services must carry out children's access assessments by 16 April 2025 as set out in our Children's Access Assessments Guidance.

5.125 Where Part 3 service providers are already using age assurance, they should also refer to the Part 3 HEAA Guidance to understand whether it is highly effective.

[567] Meta response to our May 2024 Consultation, p.7.
[568] Yoti response to our May 2024 Consultation, p.8.
[569] Section 36(4) of the Act.

A1. Legal framework: duties of providers and Ofcom in relation to the protection of children

This annex sets out the duties relating to the protection of children which are relevant to the Children's Access Assessments Guidance, Part 5 Guidance and Part 3 HEAA Guidance, published alongside this statement. As part of this annex, we also cover legal aspects relevant to human rights.

However, this annex does not cover other duties set out in the Online Safety Act 2023 ("the Act")[570], except where relevant to age assurance and children's access assessment legal framework. The legal frameworks for equality and Welsh language are set out within our impact assessment at Annex 2.

We have not referred to aspects of the legal and regulatory framework which relate to illegal content, which were covered in Annex 2 to our December 2024 Statement, which was published on 16 December 2024.[571]

Part 5 of the Act

Providers within scope of Part 5 of the Act

A1.1 Part 5 of the Act imposes specific duties on service providers that display or publish pornographic content on their online services. The duties in Part 5 of the Act apply to providers of online services containing pornographic content which:

- meets the definition of "provider pornographic content" in section 79(2) of the Act; and
- is not a category of pornographic content explicitly carved out from that definition; or
- is not otherwise exempted or excluded.

A1.2 The relevant definition in section 79(2) applies where pornographic content is published or displayed on an online service by the provider of the service, or by a person acting on behalf of the provider.

A1.3 The Act provides examples of when pornographic content will be treated as published or displayed by the provider of a service. These include where the content is:

[570] Online Safety Act 2023.
[571] Ofcom, 2024. Protecting people from illegal harms online, see Annex 2.

- published or displayed on the service by means of a software or an automated tool or algorithm applied, or made available, by the provider or a person acting on behalf of the provider;
- generated on the service by means of an automated tool or algorithm in response to a prompt by a user and is only visible or audible to that user (no matter for how short a time) (i.e. Gen AI);
- only visible or audible to users as a result of interacting with content that is blurred, distorted or obscured (for example, by clicking on the content), provided it is present on the service in question; or
- embedded on the service.[572]

Exemptions and exclusions from the scope of Part 5 of the Act

A1.4 The following types of pornographic content are excluded from the definition in section 79(2) and are therefore outside the scope of Part 5 of the Act:

- user-generated content within the meaning of section 55(3) and (4) of the Act in relation to an internet service;[573]
- text, including text accompanied by a GIF (provided that is not pornographic), an emoji or other symbol;[574]
- paid-for advertisements (as defined in section 236 of the Act);[575]
- content appearing in the search results of a search engine or a combined service.[576]

A1.5 In addition, Part 5 does not apply to on-demand programme services within the meaning of section 368A of the 2003 Act. On-demand programme services are regulated under Part 4A of the 2003 Act.[577]

Service has links with the United Kingdom

A1.6 A service will only fall within the scope of Part 5 of the Act if it has a significant number of UK users, or if UK users form one of the target markets for the service (or the only target market).[578]

Duties applying to providers within scope of Part 5

A1.7 The Act imposes the following duties on service providers that fall within the scope of Part 5:

[572] Section 79(2) and (6)(a) of the Act.
[573] Section 79(7) of the Act. Providers of U2U services on which such content appears will be subject to obligations under Part 3 of the Act, including the children's risk assessment and safety duties in sections 11 and 13 of the Act.
[574] Section 79(4) of the Act.
[575] Section 79(5) of the Act.
[576] Section 79(6)(b) of the Act.
[577] Section 80(6) of the Act. There are also certain exemptions in Schedule 1 and Schedule 9 to the Act. The principal effect of these is to exempt internal business services, such as intranets, from the scope of Part 5.
[578] Section 80(2) and (4) of the Act.

a) a duty to ensure, by the use of age verification or age estimation (or both), that children are not normally able to encounter content that is regulated provider pornographic content in relation to a service. The age assurance must be of such a kind, and used in such a way, that it is highly effective at correctly determining whether or not a particular user is a child; (***the age assurance duties***)[579] and

b) a duty to make and keep a written record, in an easily understandable form, of –

- the kinds of age verification or age estimation used, and how they are used, and
- the way in which the service, when deciding on the kinds of age verification or age estimation and how they should be used, has had regard to the importance of protecting UK users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a regulated service;[580] and
- a duty to summarise the written record in a publicly available statement, so far as the record concerns compliance with the duty to use age verification, age estimation (or both),[581] including details about which kinds of age verification or age estimation a service is using and how they are used (***the record-keeping duties***).[582]

Ofcom's duties under Part 5

A1.8 The Act requires Ofcom to produce guidance for service providers to assist them in complying with the age assurance and record-keeping duties.[583]

A1.9 The guidance must include –

- examples of kinds and uses of age verification and age estimation that are, or are not, highly effective at correctly determining whether or not a particular user is a child;
- examples of ways in which a provider may have regard to the importance of protecting users pursuant to section 81(4)(b) of the Act;
- principles that Ofcom proposes to apply when determining whether a provider has complied with each of the duties set out in section 81 of the Act; and
- examples of circumstances in which Ofcom is likely to consider that a provider has not complied with each of those duties. [584]

A1.10 The Act states that the guidance may elaborate on the following principles governing the use of age assurance for the purpose of compliance with the duty set out in section 81(2) of the Act –

a) the principle that age verification and age estimation should be easy to use;

---

[579] Section 81(2) of the Act.
[580] "including, but not limited to, any such provision or rule of law concerning the processing of personal data," section 81(4)(b) of the Act.
[581] Section 81(2) and (5) of the Act.
[582] Section 81(5) of the Act.
[583] Section 82 of the Act.
[584] Section 82(2) of the Act.

b) the principle that age verification and age estimation should work effectively for all users, regardless of their characteristics or whether they are members of a certain group;
c) the principle of interoperability between different kinds of age verification or age estimation.[585]

A1.11 The Act also states that the guidance may refer to industry or technical standards for age verification or age estimation (where they exist).[586]

Part 3 of the Act

U2U and search services in scope of the Act

A1.12 Section 3(1) of the Act defines a "user-to-user service" ("U2U") as "an internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or users, of the service". User content is known as user-generated content or 'UGC'.[587]

A1.13 A search engine is a service or functionality that enables users to search more than one website and/or database or, in principle, to search all websites and/or databases.[588]

A1.14 U2U services and search services will be in scope of the Act if they have 'links with the UK' and are not exempt.[589] The Act defines a U2U or search service as having links to the UK if it meets any one or more of the following criteria:

a) has a significant number of UK users; or
b) has UK users as one of its (or sole) target markets; or
c) is capable of being used by UK users, and there are reasonable grounds to believe there is a material risk of significant harm to UK users.[590]

A1.15 Regulated U2U and search services are together referred to as Part 3 services, per the definition set out in the Act.[591]

Duties in Part 3 of the Act: Children's access assessments

A1.16 The duties for children's access assessments apply to regulated U2U and search services (i.e. 'Part 3 services').[592]

---

[585] Section 82(3) of the Act.
[586] Section 82(4) of the Act.
[587] Section 55(3) of the Act defines "user-generated content", as content "(a) that is: (i) generated directly on the service by a user of the service, or (ii) uploaded to or shared on the service by a user of the service, and (b) which may be encountered by another user, or other users, of the service by means of the service."
[588] "Search engine" is defined in section 229 of the Act.
[589] The applicable exemptions are set out in Schedule 1 to the Act. For more information about these see [Overview of regulated services]
[590] "Regulated service" is defined under sections 4(5) and 4(6) of the Act.
[591] Section 4(3) of the Act.
[592] Section 36(1) of the Act.

A1.17 A children's access assessment first involves determining whether it is possible for children in the UK to access all or part of the service.[593] [594] The Act provides that a service can only conclude that it is *not* possible for children in the UK to access the service[595] if age verification or age estimation is used on the service with the result that children are ordinarily prevented from accessing the service.[596]

A1.18 If a provider determines that it is possible for children in the UK to access all or part of the service, the provider must go on to consider whether the child user condition is met in relation to all or the relevant part of that service.[597] That will be the case where:

a) there are a significant number of children in the UK who are users of the service or of the relevant part of it, or
b) the service, or the relevant part of it, is of a kind likely to attract a significant number of users who are children in the UK.[598]

A1.19 In relation to limb (a), the Act provides that whether or not the test is met should be assessed using evidence about actual users (and not who the intended users are).[599] If the number of users that are children in the UK is significant in proportion to the total number of UK users of the service (or the relevant part of it), then the number of children in the UK who are users is significant.[600]

A1.20 Providers who provide more than one U2U or search service must carry out a separate children's access assessment for each service.[601]

A1.21 Part 1 of Schedule 3 to the Act specifies the deadline by which providers must complete their first children's access assessment. Providers of services that start up or otherwise become Part 3 services after the publication of Ofcom's Children's Access Assessments Guidance must complete their first children's access assessment within three months of becoming a Part 3 service.[602]

A1.22 If, having conducted a children's access assessment, a provider determines that a service (or the relevant part of it) is *not* likely to be accessed by children, then it must carry out a further children's access assessment no more than one year later.[603] Such a provider is also required to carry out a further assessment:

a) before making any significant change to any aspect of the service's design or operation to which such an assessment is relevant;

---

[593] Sections 35(1)(a) and 35(5)(a) of the Act.
[594] Services do not need to assess whether parts of the service which are not, or are not included in, the U2U part of the service or a search engine can be accessed by children in the UK. See section 35(5)(b) of the Act.
[595] Or the relevant part of the service, as applicable.
[596] Section 35(2) of the Act.
[597] Section 35(1)(b) of the Act.
[598] Section 35(3) of the Act.
[599] Section 35(4)(b) of the Act.
[600] Section 35(4)(a) of the Act.
[601] Section 36(5) of the Act.
[602] Different provisions apply to providers of video-sharing platform (VSP) services currently regulated by Part 4B of the 2003 Act. These providers must complete the first children's access assessment relating to those services by the deadline specified in Part 3 of Schedule 3.
[603] Section 36(3) of the Act.

b) in response to evidence about reduced effectiveness of age verification or age estimation that is used on the service in order to achieve the result that children are not normally able to access the service;[604] or
c) in response to evidence about a significant increase in the number of children using the service.[605]

A1.23 Ofcom is required to issue guidance for U2U and search services to assist with completing the children's access assessment.[606]

A1.24 Section 37 of the Act sets out when a service will be treated as likely to be accessed by children for the purposes of the Act.

a) First, this will be the case where a children's access assessment carried out by the provider of the service concludes that it is possible for children in the UK to access all or part of the service and the child user condition is met.[607] In that case, the service will be treated as likely to be accessed by children from the date on which the children's access assessment is completed.[608]
b) Second, this will be the case where the provider of the service fails to carry out the first children's access assessment by the deadline specified in Schedule 3 to the Act.[609] In that case, the service will be treated as likely to be accessed by children from the date by which the assessment should have been completed until the first children's access assessment has been completed.[610]
c) Third, the Act provides that in specific circumstances Ofcom can take action which will result in a service being treated as likely to be accessed by children for the purposes of the Act. This will be the case where, following an investigation into the failure to complete a children's access assessment in accordance with the relevant requirements,[611] Ofcom determine that it is possible for children in the UK to access the service (or the relevant part of it) and the child user condition is met in relation to the service (or the relevant part of it)[612] and, as such mandate that the children's safety duties must be complied with by the service. In that case, the service will be treated as likely to be accessed by children from the date specified by Ofcom.[613] Ofcom has the

[604] See section 35(2) of the Act.
[605] Section 36(4) of the Act.
[606] Section 52(3)(b) of the Act.
[607] Section 37(2) of the Act.
[608] Section 37(3) of the Act.
[609] Section 37(4) of the Act.
[610] Section 37(5) of the Act. If the conclusion of that assessment is that it is possible for children in the UK to access all or part of the service and the child user condition is met then the service will continue to be treated as likely to be accessed by children by virtue of section 37(2) of the Act.
[611] Such a failure may arise either in circumstances in which no children's access assessment has been completed at all or in circumstances in which an assessment has been completed but the relevant requirements have not been complied with, for example because the assessment that has been completed is not suitable and sufficient.
[612] Sections 135(4) and 135(5) of the Act give Ofcom the power to make such a determination.
[613] The date will be specified in a confirmation decision given to the provider of the service under sections 132 and 135 of the Act.

power to specify the circumstances in which the service will cease to be treated as likely to be accessed by children.[614]

Part 3 Children's risk assessment and safety duties

A1.25 Providers of regulated U2U and search services that are likely to be accessed by children have to comply with children's risk assessment duties and children's safety duties, as well as a number of other duties. As explained below, Ofcom is required to issue Codes of Practice setting out recommended measures for complying with these duties. In this statement, Ofcom is not reaching final decisions on its recommended measures set out in our draft Protection of Children Codes (including measures relating to age assurance, which are referred to in the Part 3 HEAA Guidance). We will instead set these out in our April statement. However, for completeness, we summarise the applicable legal framework relating to these duties below.

Risk assessment duties

A1.26 Providers of regulated U2U and search services that are likely to be accessed by children have a duty to carry out a suitable and sufficient children's risk assessment[615] at the specific times set out in Schedule 3 to the Act.[616] The risk assessments must cover certain matters,[617] must be kept up-to-date up to date, including when Ofcom makes a significant change to a relevant risk profile[618] and before making any significant changes to any aspect of a service's design or operation.[619]

Children's safety duties

A1.27 Providers of regulated U2U services likely to be accessed by children have specific safety duties in relation to children's online safety as set out under section 12 of the Act. These duties extend to such parts of a service as it is possible for children to access.[620] The duties are as follows:

a) A duty, in relation to a service, to take or use proportionate measures relating to the design or operation of the service to effectively—

- mitigate and manage the risks of harm to children in different age groups, as identified in the most recent children's risk assessment of the service (see section 11(6)(g)) of the Act), and

[614] Section 135(5)(b) of the Act. The circumstances will be specified in a confirmation decision given to the provider of the service under sections 132 and 135 of the Act.
[615] Section 11(2) and 28(2) of the Act.
[616] The deadline for completing the first risk assessment depends on the day on which a provider of a U2U or search service starts its operations. See Schedule 3 to the Act.
[617] These are set out in section 11(6) and 28(5) of the Act.
[618] Section 11(3) and 28(3) of the Act.
[619] Section 11(4) and 28(4) of the Act.
[620] Section 13(5) of the Act. A provider is only entitled to conclude that it is not possible for children to access a service, or a part of it, if age verification or age estimation is used on the service with the result that children are not normally able to access the service or that part of it – see section 13(6) of the Act.

- mitigate the impact of harm to children in different age groups presented by content that is harmful to children present on the service.[621]

b) A duty to operate a service using proportionate systems and processes designed to—

- prevent children of any age from encountering, by means of the service, primary priority content that is harmful to children.[622] This duty requires a provider to use age verification or age estimation (or both) that is of such a kind, and used in such a way, that it is highly effective at correctly determining whether or not a particular user is a child, to prevent children of any age from encountering primary priority content that is harmful to children which the provider identifies on the service,[623] except where:
  - > a term of service indicates (in whatever words) that the presence of that kind of primary priority content that is harmful to children is prohibited on the service, and
  - > that policy applies in relation to all users of the service.[624]
- protect children in age groups judged to be at risk of harm from other content that is harmful to children[625] (or from a particular kind of such content), as assessed by the provider of a service in the most recent children's risk assessment of the service,[626] from encountering it by means of the service.[627]

c) A duty to include provisions in the terms of service specifying—

- how children of any age are to be prevented from encountering primary priority content that is harmful to children (with each kind of primary priority content separately covered);
- how children in age groups judged to be at risk of harm from priority content that is harmful to children (or from a particular kind of such content), as assessed by the provider of a service in the most recent children's risk assessment of the service,[628] are to be protected from encountering it, where they are not prevented from doing so (with each kind of priority content separately covered);
- how children in age groups judged to be at risk of harm from non-designated content that is harmful to children (or from a particular kind of such content), as assessed by the provider of a service in the most recent children's risk assessment

[621] Section 12(2) of the Act.
[622] Primary priority content is defined in section 61 of the Act. In summary it comprises pornographic content and content which encourages, promotes or provides instructions for: (a) suicide; (b) an act of deliberate self-injury; and (c) an eating disorder or behaviours associated with an eating disorder.
[623] Section 12(4) of the Act.
[624] Sections 12(4)-(6) of the Act.
[625] This includes priority content as defined in section 62 of the Act. In summary it comprises abusive content and content which incites hatred based on specified characteristics; violent content; bullying content; and content relating to dangerous stunts or challenges or physically harmful substances. It also includes 'non-designated content' as defined in section 60(2)(c) of the Act which is content of a kind which presents a material risk of significant harm to an appreciable number of children in the UK (subject to certain exclusions).
[626] Section 13(3) of the Act.
[627] Section 12(3) of the Act.
[628] Section 13(3) of the Act.

of the service,[629] are to be protected from encountering it, where they are not prevented from doing so.[630]

d) A duty to apply the above provisions of the terms of service consistently.[631]

e) If a provider takes or uses a measure designed to prevent access to the whole of the service or a part of the service by children under a certain age, a duty to—

- include provisions in the terms of service specifying details about the operation of the measure, and
- apply those provisions consistently.[632]

f) A duty to include provisions in the terms of service giving information about any proactive technology used by a service for the purpose of compliance with a duty set out in sections 12(2) and (3) (including the kind of technology, when it is used, and how it works).[633]

g) A duty to ensure that the provisions of the terms of service as required under sections 12(9), 12(11) and 12(12) are clear and accessible.[634]

A1.28 The duties set out in sections 12(2) and (3) of the Act apply across all areas of a service, including the way it is designed, operated and used as well as content present on the service, and (among other things) require the provider of a service to take or use measures in the specific areas, if it is proportionate to do so.[635]

A1.29 Age verification or age estimation to identify who is or is not a child user or which age group a child user is in are examples of measures which (if not required by section 12(4) of the Act may be taken or used (among others) for the purpose of compliance with the section 12(2) and (3) duties.

A1.30 Providers of regulated search services likely to be accessed by children also have specific safety duties in relation to children's online safety as set out under section 29 of the Act. These duties extend to such parts of a service as it is possible for children to access.[636] The duties are as follows:

---

[629] Section 13(3) of the Act.
[630] Section 12(9) of the Act.
[631] Section 12(10) of the Act.
[632] Section 12(11) of the Act.
[633] Section 12(12) of the Act.
[634] Section 12(13) of the Act.
[635] Namely: regulatory compliance and risk management arrangements, design of functionalities, algorithms and other features, policies on terms of use, policies on user access to the service or to particular content present on the service, including blocking users from accessing the service or particular content, content moderation, including taking down content, functionalities allowing for control over content that is encountered, especially by children, user support measures, and staff policies and practices. See section 12(8) of the Act.
[636] A provider is only entitled to conclude that it is not possible for children to access a service, or a part of it, if age verification or age estimation is used on the service with the result that children are not normally able to access the service or that part of it – see sections 30(5) and (6) of the Act.

a) A duty, in relation to a service, to take or use proportionate measures relating to the design or operation of the service to effectively—

- mitigate and manage the risks of harm to children in different age groups, as identified in the most recent children's risk assessment of the service (section 28(5)(e) of the Act), and
- mitigate the impact of harm to children in different age groups presented by content that is harmful to children present on the service.[637]

b) A duty to operate a service using proportionate systems and processes designed to:

- minimise the risk of children of any age encountering search content that is primary priority content that is harmful to children.
- minimise the risk of children in age groups judged to be at risk of harm from other content that is harmful to children (or from a particular kind of such content), as assessed by the provider of a service in the most recent children's risk assessment of the service, encountering search content of that kind.[638]

c) A duty to include provisions in a publicly available statement specifying how children are to be protected from search content of the following kinds –

- Primary priority content that is harmful to children (with each kind of primary priority content separately covered),
- Priority content that is harmful to children (with each kind of priority content separately covered) and
- Non-designated content that is harmful to children.[639]

d) A duty to –

- Include provisions in a publicly available statement giving information about any proactive technology used by a service for the purpose of compliance with a duty to include provisions in a publicly available statement giving information about any proactive technology used by a service for the purpose of compliance with a duty set out at (a) or (b) above (including the kind of technology, when it is used, and how it works;[640] and
- Ensure that the provisions of that public statement are clear and accessible.[641]

A1.31 The duties set out in sections 29(2) and (3) of the Act apply across all areas of a service, including the way the search engine is designed, operated and used as well as search content of the service, and (among other things) require the provider of a service to take or use measures in the following areas, if it is proportionate to do so.[642]

---

[637] Section 29(2) of the Act.
[638] Section 29(3) of the Act.
[639] Section 29(5) of the Act.
[640] Section 29(7) of the Act.
[641] Namely: regulatory compliance and risk management arrangements, design of functionalities, algorithms and other features relating to the search engine, functionalities allowing for control over content that is encountered in search results, especially by children, content prioritisation, user support measures, and staff policies and practices. See section 29(8) of the Act.
[642] Section 29(4) of the Act.

A1.32 Providers of regulated U2U and search services that are likely to be accessed by children are also subject to "additional duties" which are relevant, among other things, to the protection of children. These additional duties are, in brief, as follows:

a) Duties about content reporting about using systems and processes that allow users and 'affected persons' to easily report certain types of content, including content that is harmful to children;[643]
b) Duties about complaints procedures about operating a complaints procedure that allows certain relevant kinds of complaint to be made;[644]
c) Duties about freedom of expression and privacy, which concern, when deciding on and implementing safety measures and policies having particular regard to the importance of protecting users' rights to freedom of expression within the law, and importance of protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a U2U service (including, but not limited to, any such provision or rule concerning the processing of personal data);[645] and
d) Record-keeping and review duties.[646]

Protection of Children Codes

A1.33 Ofcom must issue Codes for regulated U2U and search services containing measures recommended for the purposes of compliance with certain duties including:

a) the protection of children safety duties in sections 12 and 29;[647]
b) the content reporting duties in sections 20 and 31;[648]
c) the complaints procedure duties in sections 21 and 32.[649]

A1.34 Schedule 4 to the Act sets out general principles and online safety objectives which the Codes must follow, as well as what content must be included. These are briefly summarised below.

A1.35 The Act sets out that Ofcom must consider the appropriateness of the measures we recommend to different kinds and sizes of services and to providers of differing sizes and capacities.[650] We must also have regard to the principles that:

a) Providers must be able to understand which measures apply to their service;
b) The measures must be sufficiently clear, and at a sufficiently detailed level, that providers understand what they entail in practice;
c) The measures must be proportionate and technically feasible; and
d) The measures that apply to services of various kinds and sizes must be proportionate to our assessment of the risk of harm presented by services of that kind or size.[651]

[643] Sections 20 and 31 of the Act.
[644] Sections 21 and 32 of the Act.
[645] Sections 22 and 33 of the Act.
[646] Sections 23 and 34 of the Act.
[647] Sections 41(3) and 41(10)(b) of the Act.
[648] Sections 41(3) and 41(10)(f) of the Act.
[649] Sections 41(3) and 41(10)(g) of the Act.
[650] The Act, Schedule 4, paragraph 1
[651] The Act, Schedule 4, paragraphs 2(a)-(d).

A1.36 We must also ensure that the measures described in the Codes are compatible with pursuit of a list of online safety objectives[652] and that we include measures relating to each of the areas specified in sections 12(8) and 27(4).[653]

A1.37 Any measures described in a Code of Practice must be designed in the light of, and where appropriate incorporate safeguards for the protection of, the following principles:

a) the importance of protecting the right of users and (in the case of search services or combined services) interested persons to freedom of expression within the law, and
b) the importance of protecting the privacy of users.[654]

A1.38 In deciding whether to recommend the use of age assurance, or which kinds of age assurance to recommend, in a code of practice as a measure recommended for the purpose of compliance with any of the duties set out in sections 12(2) and (3) or sections 29(2) or (3) Ofcom must also have regard to the following principles:

a) the principle that age assurance should be effective at correctly identifying the age or age-range of users;
b) relevant standards set out in the latest version of the code of practice under section 123 of the Data Protection Act 2018 (age-appropriate design code);
c) the need to strike the right balance between:
    - the levels of risk and the nature, and severity, of potential harm to children which the age assurance is designed to guard against, and
    - protecting the right of users and (in the case of search services or the search engine of combined services) interested persons to freedom of expression within the law;
d) the principle that more effective kinds of age assurance should be used to deal with higher levels of risk of harm to children;
e) the principle that age assurance should be easy to use, including by children of different ages and with different needs;
f) the principle that age assurance should work effectively for all users regardless of their characteristics or whether they are members of a certain group;
g) the principle of interoperability between different kinds of age assurance.[655]

A1.39 Providers of a regulated U2U or search service who take or use the measures described in a Code of Practice which are recommended for the purpose of complying with a relevant duty

[652] The Act, Schedule 4, paragraph 3. These differ for regulated U2U and search services.
[653] The Act, Schedule 4, paragraph 9(2) and (4). This only applies to the extent compatible with the principles set out in paragraphs 2(c)-(d).
[654] This refers to protecting the privacy of users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a U2U or search service (including any provisions concerning the processing of personal data), Schedule 4, paragraph 10(3).
[655] The Act, Schedule 4, paragraphs 12(1) and (2). In addition, Schedule 4, paragraph 12 provides that if a code of practice recommends age assurance for the purpose of complying with the duties set out sections 12(2) or (3) of the Act then it must also describe measures for the purpose of complying with the duties regarding the inclusion of clear information in the terms of service in sections 12(9), 12(11) and 12(13) of the Act; and the duties regarding complaints about age assurance in sections 21(2) and 21(3) of the Act.

will be treated as having complied with that relevant duty.[656] This means they act like a 'safe harbour'.

A1.40 Service providers do not need to follow the Codes and may seek to comply with their safety duties by taking what the Act calls 'alternative measures'. Where providers take alternative measures, the Act provides that, in doing so, they must consider the importance of protecting users' rights to freedom of expression within the law and of protecting users from breaches of relevant privacy laws.[657] They must keep a record of what they have done and explain how the relevant safety duties have been met (this is part of the record keeping duties referred to above).

Human rights

A1.41 As a public authority, Ofcom must act in accordance with its public law duties to act lawfully, rationally and fairly, and it is unlawful for Ofcom to act in a way which is incompatible with the European Convention of Human Rights ('ECHR') (section 6 of the Human Rights Act 1998).

A1.42 Of particular relevance to Ofcom's functions under the Act are the right to freedom of expression (Article 10 ECHR) and the right to privacy (Article 8 ECHR).

A1.43 The right to freedom of expression includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authority. Article 10(2) of the ECHR states that this right may be restricted in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

A1.44 Decisions at both a domestic level and before the European Court of Human Rights make clear the scope for restrictions on freedom of expression is likely to be especially limited in two overlapping fields, namely political speech and on matters of public interest. Accordingly, a high level of protection of freedom of expression will normally be accorded to these types of speech, with the authorities having a particularly narrow margin of appreciation. Intellectual and educational speech and artistic speech and expression are also considered deserving of protection under Article 10, while "mere abuse" (i.e. gratuitously offensive speech that does not contribute to public debate) attracts the lowest level of protection. Hate speech is afforded no protection under Article 10.

A1.45 Article 8(1) of the ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8(2) sets out limited qualifications, stating that public authorities must not interfere with the exercise of this right unless necessary in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[656] Section 49(1) of the Act.
[657] Section 49(5) of the Act.

A1.46 Other ECHR rights which may also be relevant to Ofcom's functions under the Act are the right to freedom of thought, conscience and religion (Article 9 ECHR) and the right to freedom of assembly and association (Article 11 ECHR).

A1.47 The need for any restriction of these rights must be construed strictly and established convincingly. Any interference must be prescribed by law; pursue a legitimate aim (as set out in Articles 8(2), 9(2), 10(2) and 11(2)); and be necessary in a democratic society – in other words, it must be proportionate to the legitimate aim pursued and corresponding to a pressing social need.

A1.48 In passing the Act, Parliament has set out in legislation the interferences prescribed by law and which it has judged to be necessary in our democratic society. Of particular relevance to the duties and functions covered by this statement, these relate to the protection of children from harm they may experience on regulated services, particularly from exposure to content that is harmful to children. The relevant legitimate aims that Ofcom may act in pursuit of in the context of our functions under the Act relating to protection of children include the prevention of crime and disorder, public safety and the protection of health or morals, and the protection of the rights and freedoms of others.

A1.49 In formulating our position in our Children's Access Assessments Guidance, Part 3 HEAA Guidance and Part 5 Guidance, where we have identified the potential for interference with ECHR rights, we have carried out a careful analysis of the relevant criteria under which such an interference may be justified as proportionate. In considering whether impacts on ECHR rights are proportionate, our starting point is to recognise that Parliament has determined that regulated services must take proportionate measures to fulfil their duties to protect children from content that is harmful to them. Such measures will necessarily have an impact on the experiences of children and adults who are using these services, in particular by significantly limiting children's exposure to such content (and in some cases, seeking to prevent such exposure altogether), and by introducing some friction for adult users in how they access and use regulated services or content that is harmful to children on those services. In doing so, this could impact their rights to freedom of expression, and in some cases, their rights to freedom of religion or belief and freedom of association. This will also have an impact on services' rights to freedom of expression, in particular as to how they impart information. They will also, to some extent, have impacts on children's and adults' rights to privacy, insofar as they would require their personal data to be processed for the measures to work properly. To the extent that such interferences can be seen as a direct result of the duties imposed on services, and Ofcom, by Parliament, and are required to achieve the legitimate objective of securing adequate protections for children from harm, we consider that a substantial public interest exists in these outcomes.

A1.50 However, in line with our obligations under the Human Rights Act, we also seek to secure that any such interference with adults' and children's rights to freedom of expression and privacy, or other relevant rights, is proportionate to the legitimate objectives pursued, and where appropriate we explain why the relevant restriction is justified, and have sought to build in appropriate safeguards to protect those rights where appropriate. In doing so, among other things, we have carefully considered whether other, less intrusive measures

are available that might adequately mitigate the harms faced by children on regulated services.[658]

A1.51 Overall, we have sought to strike a fair balance between securing adequate protections for children from harm (and their rights in respect of this) and the ECHR rights of users (both children and adults), other interested persons (including for example, persons who host websites and who may be featured in content on regulated services or whose content might be on those services regardless of whether or not they may be service users) and services, as relevant.[659] In other words, we are concerned to ensure that the degree of interference with ECHR rights is outweighed by the benefits secured in terms of protecting children from harm. In seeking to achieve this fair balance, we consider that the Act and the protection it gives to individuals against harms of various kinds[660] reflect the decision of the UK Parliament that UK users, and UK child users in particular, should be proportionately protected from all the harms concerned. In doing so, Parliament has enshrined in UK law the rights of UK users – including their human rights – to be protected from those harms. In weighing up whether our approach in the decisions in this statement are proportionate, we start from the position that UK users should be protected from the harms set out in the Act.

A1.52 We note that the UK has ratified the United Nations Convention on the Rights of the Child ('UNCRC')[661] and the UK Government is required to make law that gives effect to it. Among other things, the UNCRC requires that the best interests of the child should be a primary consideration in all actions concerning children, including those taken by public authorities such as Ofcom.[662] Similarly, General comment No. 25 (2021) on children's rights in relation to the digital environment[663] explains that States parties should ensure that, in all actions regarding the regulation, design, management and use of the digital environment, the best interests of the child is a primary consideration. General comment No.25 also explains that in considering children's best interests, regard should be had to all children's rights, including their rights to seek, receive and impart information, to be protected from harm and to have their views being given due weight, and ensure transparency in the assessment of their best interests. The UK Parliament has made clear in debates during the legislative process that the spirit of the UNCRC is reflected in the Act, highlighting that the definition of 'child' as anyone under 18 aligns with that in the UNCRC and children's rights feature in the safety objectives, with a higher standard of protection against harm required for children than for adults.[664] As the wording of the UNCRC is not directly incorporated into the Act, rather than making direct reference to the UNCRC (or General comment No. 25), we consider and reference the relevant statutory duties in the Act and impacts on ECHR rights,

---

[658] This reflects the third limb of what is often referred to as the 'Bank Mellat test', as set out by Lord Reed JSC in Bank Mellat v HM Treasury (No 2) [2013] UKSC 39; [2014] AC 700.
[659] This reflects the fourth limb of the 'Bank Mellat test'
[660] Including in particular the duties aimed at protecting children from harm which are the key focus of the Children's Access Assessments Guidance and Part 5 Guidance, as well as the duties which apply to illegal content and activity covered in Ofcom's [Illegal Harms Statement].
[661] United Nation Convention on the Rights of the Child, adopted 20 November 1989 by General Assembly resolution 44/25.
[662] See Article 3 of the UNCRC
[663] General comment No. 25 of the UN Committee on the Rights of the Child, published 2 March 2021
[664] Hansard, House of Lords, 2 May 2023, Column 1463 [accessed 22 April 2024].

in line with the applicable requirements under UK domestic law, which encompasses and reflects relevant aspects of the UNCRC. In this way, our approach also encompasses, and is consistent with, relevant aspects of the UNCRC and General Comment 25, including in giving particular weight to the importance of the best interests of children in deciding on our approach within the Children's Access Assessments Guidance, Part 3 HEAA Guidance and Part 5 Guidance.

A1.53 We address the relevant rights impacts on users, services and other persons in Annex 2 in relation to for the Children's Access Assessments Guidance and Part 5 Guidance.

A2. Impact assessments

A2.1 This annex comprises three sections. First, we set out the scope of the impact assessments we have carried out in preparing this statement. Second, we assess the likely impact of the Guidance for service providers publishing pornographic content ("Part 5 Guidance"). Finally, we assess the likely impact of the Children's Access Assessments Guidance.

A2.2 The Children's Access Assessments Guidance refers to the Guidance for Part 3 services on highly effective age assurance ("Part 3 HEAA Guidance") as part of Stage 1 of the children's access assessment process. The children's access assessments impact assessment takes into account the impact of the Part 3 HEAA Guidance in this context. The Part 3 HEAA Guidance is also relevant to any measures in our Protection of Children Code for user-to-user services that refer to highly effective age assurance, which we do not consider here. Our May 2024 Consultation Protecting Children from Harms Online ("May 2024 Consultation") proposed such measures and included our impact assessment of these.[665] We will update our impact assessment and confirm our position for these measures separately in our Protection of Children statement in April 2025.

Scope of impact assessments

A2.3 In our overview of the legal framework at paragraph 2.14 of this statement, we set out Ofcom's impact assessment duties.

A2.4 In this impact assessment, we assess the likely impact of our Part 5 Guidance and Children's Access Assessments Guidance and relevant aspects of the Part 3 HEAA Guidance, which will be assessed further in our April statement. The guidance documents are intended to assist relevant providers in complying with specific duties in the Act. Those duties are detailed within Annex 1. In this impact assessment, we have not considered the impacts of the duties themselves, as service providers are under a statutory obligation to comply with these duties, over which we have no discretion. We also have not set out an impact assessment where we have made suggestions of what service providers 'may wish to consider' when complying with the duties, as these are decisions for each service provider to determine.

A2.5 Our impact assessments focus on the areas where we have exercised discretion, in terms of specifying recommended steps that providers should take to comply with the relevant duties.

A2.6 Each of the impact assessment sub-sections is structured as follows:

- First, we assess the direct impact of our guidance on service providers including small and micro businesses.
- Second, where relevant, we assess any other impacts including indirect costs which could affect the interests of consumers in these markets (only relevant in relation to the Part 5 Guidance).

[665] May 2024 Consultation on Protecting Children from Harms Online, Volume 5.

- Third, we set out our assessment of the impact of our guidance on users' rights, including freedom of expression, freedom of association, and privacy.
- Fourth, we set out our assessment of the impact of our guidance on the Welsh Language.
- Finally, we assess the impact of our guidance on persons sharing protected characteristics under the Equality Act 2010 ("EA 2010") and more generally under section 3 of the 2003 Act.

Assessing the impact of the Part 5 Guidance

A2.7 In Sections 3 and 4 of this statement, we have set out our decisions in relation to the Part 5 Guidance. We have reached those decisions after considering and assessing the likely impact of our Part 5 Guidance on the service providers who will need to comply with the age assurance duties under Part 5 of the Act. In doing so, we have also taken account of responses to our December 2023 Part 5 Consultation[666] relevant to our consideration of such impacts. This part of this annex explains how we have carried out our impact assessment in that regard.

A2.8 Our impact assessment in this sub-section focuses, in particular, on the following matters in the Part 5 Guidance that we recommend service providers should consider in complying with their Part 5 duties:

- ensure the age assurance process implemented fulfils the criteria of technical accuracy, robustness, reliability, and fairness;
- consider the principles of accessibility and interoperability when implementing age assurance;
- take appropriate steps to mitigate against methods of circumvention of the age assurance process that are easily accessible to children and where it is reasonable to assume that children may use them;
- consider whether to offer alternative methods where an age assurance method is only highly effective for a limited number of users;
- ensure that the written record is durable, accessible, easy to understand, and up-to-date;
- familiarise themselves with the data protection legislation, and how to apply it to their age assurance method(s), by consulting guidance from the ICO; and
- refrain from hosting, sharing, or permitting content that directs or encourages child users to circumvent the age assurance process or access controls.

A2.9 We have made minor changes to the Part 5 Guidance, as compared to our consultation version, largely for clarity and consistency with the Part 3 HEAA Guidance.

A2.10 We have also summarised below our assessment of the impact of our Part 5 Guidance on various stakeholders. We note that several respondents – including Barnardo's, Nexus NI, One ID, Verifymy, and Yoti – broadly supported our overall impact assessment on the draft Part 5 Guidance. Therefore, we have decided to focus below on those respondents to our

[666] Ofcom, 2023. Consultation: Guidance for service providers publishing pornographic content .

consultation who disagreed with aspects of our impact assessment on the draft Part 5 Guidance or otherwise raised specific issues.

Direct impact on regulated service providers, including small and micro businesses

Our consultation position

Overview of direct impact on service providers

A2.11 In Annex 1 of our December 2023 Part 5 Consultation, we set out our assessment of the potential direct costs that service providers could incur as a result of our proposed approach. This covered the justification for and potential benefits which may arise from our Part 5 Guidance, focusing on areas where we have exercised discretion, as well as the potential direct costs resulting from this. We summarise our consultation position in the table below.

Table A2.1: Summary of our consultation position on the impact of our Part 5 guidance on regulated service providers

Draft Part 5 guidance	Justification and potential benefits	Potential direct costs
Service providers should ensure the age assurance process implemented fulfils the criteria of technical accuracy, robustness, reliability and fairness.	For age assurance to be highly effective, as required by the Act to achieve the objective that children are not normally able to encounter pornographic content, we considered that these criteria should be fulfilled. We set out that they form part of our minimum expectations of the steps required in practice for providers to meet their duties. We set out that our criteria-based approach provides flexibility, rather than recommending a specific kind of age assurance. This should benefit providers, as it allows them to future-proof their systems and respond to their user base and technical developments over time in the most appropriate and cost-effective way for them.	There may be staff costs (internal or external) associated with understanding the criteria and assessing potential age assurance processes against the criteria. There may also be additional staff and development costs associated with reviewing and updating age assurance processes over time as technology evolves.

Draft Part 5 guidance	Justification and potential benefits	Potential direct costs
Service providers should implement effective access controls on their service to prevent users who have been identified as children through the age assurance process from encountering pornographic content on the service.	Effective access controls are necessary to achieve the objective that children are not normally able to encounter pornographic content. They formed part of our minimum expectations of the steps required in practice for providers to meet their duties. We recognised the risk of children circumventing the access controls or age assurance process. For this reason, we considered there is material benefit in recommending that providers should not host or permit content that directs or encourages child users to do so.	There may be costs arising from efforts to identify and prevent content that directs or encourages child users to circumvent the age assurance or access control method. However, the scale of this would likely be limited where there are limited content/functionalities available to users prior to the age check.
Service providers should consider the principles of accessibility and interoperability when implementing age assurance.	These principles are important to achieve the secondary policy objective to ensure that service providers' use of age assurance does not unduly prevent adult users from accessing legal pornographic content. As above, we considered there are benefits from the flexibility provided by a criteria-based approach.	There may be staff costs (internal or external) associated with understanding and considering the principles when implementing age assurance. For instance, drafting explanatory text on how the age assurance process works or assessing the impact of the age assurance process on users with different characteristics.
Service providers should ensure the written record is durable, accessible, and up to date.	We set out that these are our minimum expectations required for service providers to fulfil their record-keeping duties. For instance, to meet the duty to 'keep' a written record, we proposed that a service provider should retain written records in accordance with their record retention policies, or for a minimum of five years, whichever is longer.	There may be some costs arising from our expectations around record-keeping. For instance, there may be a minor systems infrastructure cost associated with retaining the written record for a minimum of five years, if the service provider's current record retention policies are shorter than this.

Draft Part 5 guidance	Justification and potential benefits	Potential direct costs
Service providers should familiarise themselves with the data protection legislation, and how to apply it to their age assurance method(s), by consulting ICO guidance.	We set out that these are our minimum expectations for providers to fulfil the duty to keep a written record of how they have had regard to the importance of protecting UK users from a breach of any statutory provision or rule of law concerning privacy. These expectations are also likely to be required to ensure compliance with data protection law.	There may be some staff costs associated with efforts to consult and understand the relevant ICO guidance.

A2.12 We set out in our consultation that the potential direct costs incurred by a service provider would depend on how it approaches compliance with its online safety duties and our Part 5 Guidance. For instance, service providers may incur the above costs as part of internal staff costs, or due to outsourcing to external experts or suppliers.

A2.13 In general, we assessed that some costs could be somewhat lower for smaller or less complex services. However, as we set out in Annex 1 of our December 2023 Part 5 Consultation, the overall direct costs relating to our proposed guidance are likely to be a greater proportion of the total costs/revenues for smaller firms. Regardless, the large majority of costs arise directly from the Act, which requires the implementation of highly effective age assurance, rather than any approaches we have recommended exercising our regulatory discretion in our guidance. The guidance gives service providers a degree of flexibility in how they choose to comply, which will allow them to future-proof their systems and respond to their user base and technical developments over time in the most appropriate and cost-effective way for them. We therefore concluded that the impact of our guidance on regulated service providers, including small and micro businesses, was proportionate.

Summary of responses

A2.14 One ID and Yoti broadly supported our impact assessment on service providers.[667] Multiple respondents said that the assessment was proportionate.[668] Arcom and Nexus supported the degree of flexibility that the guidance offered to service providers.[669]

A2.15 The Free Speech Coalition said that Ofcom has underestimated the costs of implementing age assurance to service providers, particularly to small and micro businesses. Further,

[667] One ID response to our December 2023 Part 5 Consultation, p.4; Yoti response to our December 2023 Part 5 Consultation, pp.19-20.
[668] Nexus response to our December 2023 Part 5 Consultation, p 5; One ID response to our December 2023 Part 5 Consultation, p.4; Verifymy response to our December 2023 Part 5 Consultation, p.7.
[669] Arcom response to our December 2023 Part 5 Consultation, p.8; Nexus response to our December 2023 Part 5 Consultation, p.5.

they provided estimates of the costs to different types of service providers.[670] One respondent said that building age assurance solutions is too costly and complex for many service providers.[671]

A2.16 The Age Verification Providers Association ("AVPA") said the age assurance industry has experienced a downward trend in pricing over the past five years due to technical innovation and increased competition, and that they expected this trend to continue and to be further affected by interoperability.[672] Yoti (a third-party age assurance provider) said that it already offers specific offers and packages to smaller organisations, which could lower their costs of implementing age assurance.[673]

A2.17 ID Crypt said that some age assurance methods, including credit card checks and photo-ID matching could be costly for service providers.[674]

Our updated impact assessment

A2.18 We have considered the consultation responses and have concluded that our assessment of impacts on service providers, including small and micro businesses that we set out in the consultation, broadly still applies. We clarify some aspects of our assessment below, where relevant to specific responses.

A2.19 In response to the comments about the overall cost of implementing age assurance, as explained in paragraph A2, we have not assessed the costs of implementing highly effective age assurance (including for small and micro businesses as well as larger ones), because this arises directly from the statutory requirement in the Act, over which we have no discretion.

A2.20 The Act requires highly effective age assurance to be in place on all services in scope, regardless of their size or the resources available to the providers. Our Part 5 Guidance reflects our expectations of the steps providers should follow in practice to meet their age assurance duties under Part 5 of the Act. Setting lower expectations for smaller services would be inconsistent with the Act and could lead to ineffective age assurance on smaller services, exposing children to significant harm. Overall, the bulk of costs, for services of all sizes, comes from the duties in the Act and we consider that our guidance will support services in complying with those duties by clarifying the steps they should take in practice.

A2.21 We acknowledge, however, that the costs summarised in Table A2.1 above which result from our Part 5 Guidance – rather than from the duties themselves – may still be material. We also recognise that these costs could represent a higher proportion of costs or revenue for smaller providers than for larger ones. Smaller service providers with few employees may, for example, have to rely on external expertise that is not readily available internally. On the other hand, smaller service providers may be more agile in implementing changes and could face less complex internal governance processes, which could reduce some of the costs involved in following our guidance. Overall, we consider that our criteria-based approach gives service providers flexibility to adopt an age assurance process that best

[670] Free Speech Coalition response to our December 2023 Part 5 Consultation, pp.8-10.
[671] Name Withheld 9 response to our December 2023 Part 5 Consultation, pp.3-4.
[672] AVPA response to our December 2023 Part 5 Consultation, pp.11-12.
[673] Yoti response to our December 2023 Part 5 Consultation, p.19.
[674] ID Crypt response to our December 2023 Part 5 Consultation, p.2.

suits their own specific contexts, and to pursue cost-effective approaches, as long as the relevant criteria are met.

A2.22 In response to ID Crypt's comments, we acknowledge that some methods of age assurance may be more costly than others. Our Part 5 Guidance is flexible and does not recommend the use of specific age assurance method(s), recognising that various methods may be capable of being highly effective.

Assessing the impact of changes to our final guidance

A2.23 We have also considered whether any of the changes made to our Part 5 Guidance (compared to the draft guidance) would materially impact service providers. Overall, our changes are limited and intended to improve clarity for service providers, which should make it easier in helping them to comply with their duties. This includes acknowledging that email-based age estimation may be capable of being highly effective and reducing the retention period for record keeping duties from five to three years.

A2.24 We recognise, however, that specific clarifications – including where we explain that service providers should consider whether repeated age checks are needed and should use a challenge age approach as part of age estimation – could have cost implications in some cases. However, we consider such impacts justified and necessary to meet the minimum expectations set out in the Act, as there is a clear and material risk that age assurance processes may not be highly effective if such steps were not followed. Therefore, we have not identified any reason to change our assessment of impacts on service providers.

Other impacts

Indirect impacts on service providers

Our consultation position

A2.25 In Annex 1 of our December 2023 Part 5 Consultation, we recognised that the duty to implement age assurance may impact service providers' user numbers, which could reduce revenue from advertising and/or subscriptions. However, we considered this risk is mitigated by the fact that (as discussed above in Table A2.1) our proposed guidance is intended to help ensure that adult users are not unduly prevented from accessing legal content. Service providers have commercial incentives to introduce age assurance in a way which seeks to minimise any avoidable negative impact on revenue. Where revenue is impacted, we considered this a result of complying with the duties themselves rather than a consequence of our approach to the Part 5 guidance.

A2.26 We did not consider that our proposed guidance would unduly affect competition in the provision of pornographic services because it applies to all Part 5 service providers. We noted that giving service providers flexibility over how to implement age assurance would allow service providers and third-party age assurance providers to develop alternative innovative age assurance methods. The requirement for all Part 5 services to implement age assurance could increase competition among third-party age assurance providers, improve quality and/or put downward pressure on prices and the cost of age assurance. This could also improve the experience of users of these services.

Summary of responses

A2.27 The Free Speech Coalition said that the cost of compliance will prompt smaller service providers to exit the market and discourage new entrants, which could entrench the

position of larger service providers.[675] Two respondents said that our measures could adversely impact competition absent a robust enforcement approach.[676]

A2.28 Barnardo's said that Ofcom should have included an assessment of the positive impacts of the policy in preventing children from accessing online pornographic content.[677]

Our updated impact assessment

A2.29 We have considered consultation responses and have concluded that our assessment of indirect impacts on service providers broadly still applies. We clarify some aspects of our assessment below, where relevant to specific responses.

A2.30 We acknowledge that the costs resulting directly from our guidance (both the direct costs of the guidance, and any indirect costs such as revenue losses) are likely to be a greater proportion of total costs/revenues for smaller firms. There is a possibility that some service providers may choose to exit the UK market or may be discouraged from entering the UK market.

A2.31 However, the large majority of costs associated with implementing highly effective age assurance result from the duties in the Act itself, over which we have no discretion. To the extent that specific recommendations in our guidance impact services, we have explained in the previous section why we consider this appropriate and proportionate, even for smaller services. To the extent that there are any indirect impacts, such as on revenues and competition, we note that our approach provides flexibility in how to implement age assurance, which should mitigate adverse impacts. More prescriptive recommendations, which might be well suited to some services but not others could risk distorting competition. Therefore, we conclude that any wider competition and market impacts of our guidance are proportionate and justified.

A2.32 In response to comments from stakeholders about not enforcing swiftly and equally across the whole sector, we recognise the risk that users may seek to move to services that do not use age assurance. The timings of implementation of the regime are set by Government, not Ofcom. We will take steps to monitor compliance with the Part 5 duties to use highly effective age assurance to prevent children from encountering pornographic content and to monitor compliance with the equivalent duties on Part 3 U2U services that allow pornographic content when they come into force. We will be investing in public awareness campaigns to encourage adults to engage with age assurance rather than visit sites that may be less safe.

A2.33 In response to Barnardo's comments, we do not assess in detail or quantify the benefit of children being prevented from accessing these services, since this outcome is required by the Act itself. However, we explicitly consider the importance of supporting this outcome in our impact assessment, e.g., in the potential benefits summarised in Table A2.1. We also reflect the harms that children experience from pornographic content as part of our Register of Risks which we will finalise alongside our Protection of Children Statement in April.

---

[675] Free Speech Coalition response to our December 2023 Part 5 Consultation, pp.8-10.
[676] [✂]; Yoti response to our December 2023 Part 5 Consultation, p.20.
[677] Barnardo's response to our December 2023 Part 5 Consultation, p.10.

Assessing the impact of changes to our final guidance

A2.34 We believe the changes to the guidance do not materially affect this part of our assessment, and therefore we have not changed our assessment of indirect impacts on service providers on that basis.

Impact on adult users

Our consultation position

A2.35 In Annex 1 of our December 2023 Part 5 Consultation, we stated that if age assurance is not fair or accessible, it may unduly exclude adults from accessing legal content. The additional principles of accessibility and interoperability proposed in the guidance may improve the user experience of age assurance and reduce the risk that adult users are unable to access legal content. Absent our proposed principles, some users could be unable to access this content because, for example, the age assurance process might be too difficult to use resulting in some users abandoning the process. Alternatively, some users might not be able to meet the requirements, for instance if they lack the required identification documents. These recommended principles should minimise the number of legitimate users being wrongly excluded from accessing these services and this content.

A2.36 We noted that service providers are already likely to aim to maximise revenues from subscriptions and advertising, and so they should already have incentives to minimise the loss of users because of the requirement to implement age assurance, absent our proposed guidance.

A2.37 We did not consider that our proposed guidance will materially increase the costs to adult users.

Summary of responses

A2.38 Yoti stated that users should be given a choice of age assurance methods to ensure adult users are not unduly excluded from accessing legal content.[678] No other respondents commented on the impact on adult users.

Our updated impact assessment

A2.39 We have considered this consultation response and have concluded that our assessment of impacts on adult users broadly still applies. We clarify some aspects of our assessment below, where relevant to specific responses.

A2.40 Our Part 5 Guidance recommends that service providers consider the principle of accessibility when implementing age assurance. This entails ensuring that age assurance be easy to use and work effectively for all users. As set out in paragraph 4.92, service providers could consider offering users more than one age assurance method. Including multiple kinds of highly effective age assurance methods and allowing users to choose which is most appropriate to them, is one means of helping to ensure that the overall age assurance process is accessible and does not unduly exclude adult users from accessing legal content. However, service providers are not required to implement multiple kinds of age assurance and providers may be able to achieve an accessible age assurance process which is highly effective with a single age assurance method.

[678] Yoti response to our December 2023 Part 5 Consultation, p.13.

Assessing the impact of changes to our final guidance

A2.41 We have also considered whether any of the changes made to our Part 5 Guidance (compared to the draft guidance) would materially affect adult users. We note that using a 'challenge age' approach can help to improve the overall effectiveness of the age assurance process by preventing or minimising borderline cases involving errors. We do not think the changes to the guidance would have material implications for adult users in most cases.

A2.42 We acknowledge that recommending the use of challenge ages to mitigate false positives could have an impact on the rates of false negatives (adults misclassified as children) and may introduce additional friction for these users. Further, in some cases, adults may undergo additional age checks, e.g. from repeating age assurance and/or from the secondary check in a 'challenge age' approach. However, we consider such impacts justified and necessary to meet the criteria of technical accuracy. Therefore, we have not identified any reason to change our assessment of impacts on adult users.

Rights assessment

A2.43 In Annex 1, we have set out Ofcom's duties under the European Convention of Human Rights ('ECHR').[679] In carrying out our rights assessments across this statement, we have addressed the relevant rights impacts on users, services and other persons and have considered the extent to which our proposals may interfere with certain rights in the ECHR as set out in Schedule 1 of the Human Rights Act 1998. Further detail is set out in Annex 1. Where a right is engaged, the interference may be justified where it is:

- in accordance with the law;
- the law in question pursues a legitimate aim and it is proportionate to that aim; and
- there is a pressing social need.

Freedom of expression and freedom of association

A2.44 Article 10 of the ECHR sets out the right to freedom of expression, which encompasses the right to hold opinions and to receive and impart information and ideas without unnecessary interference by a public authority. Article 11 sets out the right to associate with others. We must exercise our duties under the Act in light of users' and services' Article 10 and 11 rights and not interfere with these rights unless we are satisfied that to do so is prescribed by law, pursues a legitimate aim, is proportionate to the legitimate aim, and corresponds to a pressing social need.

Summary of responses

A2.45 We did not receive any response which expressly cited Article 10 or 11 of the ECHR, but the Free Speech Coalition observed that the use of an 'age-gate' may cause some friction in terms of access to these regulated services which may deter some users,[680] while other

[679] Human Rights Act 1998 c.42.
[680] Free Speech Coalition response to our December 2023 Part 5 Consultation, p.5.

users may be incorrectly identified as underage and therefore barred from accessing the site.

Our final rights assessment

A2.46 Further to consideration of responses to consultation, we have not made changes to our rights assessment for our Part 5 Guidance in respect to the rights to freedom of expression and association.

A2.47 The age assurance duties require service providers to ensure that children are not normally able to encounter pornographic content. We therefore believe that our criteria-based approach has a limited impact on freedom of expression, in so far as service providers are free to implement different forms of age assurance, including age verification or age estimation, which is suitable for their platform and user base provided it is highly effective in determining if the user is a child. We have also made recommendations on the principle of accessibility to ensure adults are not unduly excluded from accessing legal content. They are not required to alter or modify their content or the design of their service. Taken together we believe our approach is proportionate to the aims of the Act, bearing in mind the policy objective is to protect children from accessing pornographic content.

Privacy

A2.48 Article 8 of the ECHR sets out the right to respect an individual's private and family life. The use of an age assurance process to determine if a user is a child will involve the collection and processing of personal data.

Summary of responses

A2.49 The ICO expressed support for the approach taken in the Part 5 Guidance. They stated that under data protection law, services must ensure that the amount of personal information they collect about a person to verify or assure their age is proportionate. Where less intrusive – but still highly effective – methods are available, they should be used.[681]

A2.50 Some respondents expressed concern about the amount of personal data that would be collected and processed as a result of providers implementing an age assurance process.[682]

---

[681] ICO response to Part 5 Consultation, p.3.

[682] [✂]; Association of Police and Crime Commissioners response to our May 2024 Consultation, p.3; Big Brother Watch response to our May 2024 Consultation, pp.22-23; Burville, M response to our December 2023 Part 5 Consultation, pp.1-3; Collier D, response to our December 2023 Part 5 Consultation, pp.1-3; Free Speech Coalition response to December 2023 Part 5 Consultation, p.7; Fringe Dweller Productions response to our December 2023 Part 5 Consultation, pp.1-3; Global Network Initiative response to our May 2024 Consultation, pp.4-5; Mega Limited response to our May 2024 Consultation, p.14; Hutchison, A response to our December 2023 Part 5 Consultation, p 2-3; Jackson, EM response to our December 2023 Part 5 Consultation, p 2-3; ID Crypt Global response to December 2023 Part 5 Consultation, p.1; Name withheld 9 response to our December 2023 Part 5 Consultation, p.3; Mid Size Platform Group response to our May 2024 Consultation, p.3; Pinterest response to our May 2024 Consultation, p.12; Integrity Institute response to our May 2024 Consultation, pp.2-3; Northern Ireland Commissioner for Children and Young People (NICCY) response to May 2024 Consultation, p.31; Name Withheld 8 response to our December 2023 Part 5 Consultation, pp.2-3; Name Withheld 1 response to our December 2023 Part 5 Consultation, pp. 1-3; Name Withheld 2 response to our December 2023 Part 5 Consultation, pp.2-3; Name Withheld 3 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 4 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 5 response

5Rights argued that Ofcom should include 'privacy preserving' in the criteria, on the basis that this would mandate that services have privacy and security built into their processes.[683] They also suggested that the criteria must include a requirement that age assurance process must only use information necessary for establishing the age of the user and delete this information once it has confirmed the age of the user.[684]

A2.51 Big Brother Watch and the Integrity Institute warned about the risk of data leaks generally.[685] Other respondents expressed concern about the privacy implications of specific methods of age assurance, for example, ACT - The App Association suggested that hard identifiers (such as photo-ID matching) are unnecessarily intrusive because they contain more personal information than is needed to determine the age of a user.[686] Open Rights Group raised concerns around the privacy risks associated with age verification.[687]

Our final rights assessment

A2.52 In response to stakeholder concern around data protection and privacy, we have made the following minor amendments to our Part 5 guidance:

a) We have incorporated references in our Part 5 Guidance to applicable ICO guidance on data protection legislation to assist services when implementing their preferred age assurance method to enable them to comply with data protection legislation.

b) We have amended the recommendation that providers retain a written record of the outcome of individual age checks for a period of three years (calendar or financial, whichever is longer) rather than the five years as proposed in the draft Part 5 Guidance.

A2.53 The impact of these minor amendments does not change the outcome of our rights assessment in regards to privacy and data protection. We consider that it strengthens our conclusion that our Part 5 Guidance will not disproportionately impact upon users' rights to privacy and can be achieved in a manner compliant with data protection legislation.

A2.54 The Part 5 Guidance makes it clear that service providers should follow a data protection by design approach when implementing their preferred age assurance method so that they comply with data protection legislation. To assist service providers, we have incorporated references to applicable ICO guidance on data protection legislation in the Part 5 Guidance.

A2.55 Provided service providers adopt a highly effective age assurance process, in accordance with our recommended criteria, they may choose an age assurance process which minimises the amount of personal data collected. This will ensure that adult users are not subjected to overly intrusive processes when accessing legal content and are not

---

to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 6 response to our December 2023 Part 5 Consultation, pp.1-3; Safazadeh, S, response to our December 2023 Part 5 Consultation, pp.1-3; Shaw, A. response to our December 2023 Part 5 Consultation, pp.1-3; Warren A, response to our December 2023 Part 5 Consultation, pp.2-4; xHamster response to our December 2023 Part 5 Consultation, p.3; xHamster response to our May 2024 Consultation, p.2; 14 further confidential individual respondents to our December 2023 Part 5 Consultation, pp.1-4.

[683] 5Rights response to Part 5 consultation, p.2.

[684] 5Rights response to Part 5 consultation, p.6.

[685] Big Brother Watch response to our May 2024 Consultation, p.22; Integrity Institute response to our May 2024 Consultation, p.2.

[686] ACT - The App Association response to our May 2024 consultation, pp.2-3.

[687] Open Rights Group response to Illegal Harms Consultation, p.7.

disproportionately impacted. We believe this approach is proportionate to the aim of Part 5, namely to have processes in place to stop children encountering pornographic content.

A2.56 We would remind service providers that they are required, under the Act, to keep and maintain a written record explaining how the age assurance used is highly effective at determining if a user is a child and how they have had regard to privacy and data protection legislation. We have exercised our regulatory discretion and made a number of recommendations to assist service providers to comply with this requirement in a manner which ensures that only necessary data is retained for the purposes of retaining a written record. For example, we have explained in the Part 5 Guidance that service providers do not need to keep a record of the outcome of individual age checks and we have also recommended that the written record is retained for a minimum of three years (either calendar or financial), whichever is longer (rather than five years as proposed in the draft Part 5 Guidance).

A2.57 We believe that our approach to implementing HEAA and the record keeping duties will assist service providers to limit the extent of any interference with a user's right to privacy while enabling them to comply with their legal requirements. These measures are proportionate to the aim of the Act which is to ensure that children are not normally able to encounter pornographic content.

Welsh Language Impact Assessment

Welsh language legal framework

A2.58 The Welsh language has official status in Wales. To give effect to this, certain public bodies, including Ofcom, are required to comply with the Welsh language standards.[688]

A2.59 The Welsh Language (Wales) Measure 2011 made the Welsh language an officially recognised language in Wales. This legislation also led to the establishment of the Office of the Welsh Language Commissioner who regulates and monitors our work. Ofcom is required to take Welsh language considerations into account when formulating, reviewing or revising policies which are relevant to Wales (including proposals which are not targeted at Wales specifically but are of interest across the UK).[689]

A2.60 Accordingly, we have considered:

a) The potential impact of our policy proposals on opportunities for persons to use the Welsh language;

b) The potential impact of our policy proposals on treating the Welsh language no less favourably than the English language; and

c) How our proposals could be formulated so as to have, or increase, a positive impact, or not to have adverse effects or to decrease any adverse effects.

[688] The Welsh language standards with which Ofcom is required to comply are available on our website.
[689] See Standards 84-89 of Hysbysiad cydymffurfio (in Welsh) and compliance notice (in English). Section 7 of the Welsh Language Commissioner's Good Practice Advice Document provides further advice and information on how bodies must comply with the Welsh Language Standards.

Our consultation position

A2.61 In Annex 1 of our December 2023 Part 5 Consultation, we considered that setting out that service providers can keep their written records in English or Welsh where the provider is based in Wales will have a positive effect on opportunities to use the Welsh language and on the equal treatment of Welsh and English.

A2.62 We did not propose any specific language requirement in relation to age assurance process or the statutory duty to make a publicly available statement other than that they should be accessible. This leaves it open to service providers to decide what language is appropriate, including whether to provide a Welsh language version of the age assurance process or publicly available statement if, in particular, the service is targeted at Wales or Welsh speakers. For these reasons, we considered that our policy proposals will have positive effects on opportunities to use Welsh and on treating Welsh no less favourably than English. We did not consider that there is scope, acting within our powers, to formulate our proposed guidance differently so as to have increased positive effects on these matters.

Summary of responses

A2.63 Nexus NI and Te Mana Whakaatu expressed support for our Welsh Language Impact Assessment.[690]

A2.64 The Age Verification Providers Association said that it would expect its members to provide their services, and the notices that explain them, in Welsh (as well as English) where they are accessed by users located in Wales.[691]

Our updated assessment

A2.65 We have considered the consultation responses and changes to the guidance (compared to the draft guidance) and have not identified any reason to change our Welsh Language Impact Assessment. We note the response from the Age Verification Providers Association and still consider it appropriate to allow service providers flexibility with respect to language as part of our accessibility principle.

Equality Impact Assessment

Equality legal framework

A2.66 Section 149 of the Equality Act 2010 ('the 2010 Act') imposes a duty on Ofcom, when carrying out its functions, to have due regard to the need to eliminate discrimination, harassment, victimisation and other prohibited conduct related to the following protected characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex and sexual orientation.

A2.67 The 2010 Act also requires Ofcom to have due regard to the need to advance equality of opportunity and foster good relations between persons who share specified protected characteristics and persons who do not.

[690] Nexus response to our December 2023 Part 5 Consultation, p.5; Te Mana Whakaatu response to our December 2023 Part 5 Consultation p.4.
[691] AVPA response to our December 2023 Part 5 Consultation, p.12.

A2.68 Section 75 of the Northern Ireland Act 1998 ('the 1998 Act') also imposes a duty on Ofcom, when carrying out its functions relating to Northern Ireland, to have due regard to the need to promote equality of opportunity and have regard to the desirability of promoting good relations across a range of categories outlined in the 1998 Act. Ofcom's Revised Northern Ireland Equality Scheme explains how we comply with our statutory duties under the 1998 Act.[692]

A2.69 To help us comply with our duties under the 2010 Act and the 1998 Act, we assess the impact of our regulatory approach in relation to children's access assessments, highly effective age assurance and Part 5 duties on persons sharing protected characteristics and, in particular, whether they may discriminate against such persons or impact on equality of opportunity or good relations.

A2.70 When thinking about equality, we think more broadly than persons that share protected characteristics identified in equalities legislation and think about potential impacts on various groups of persons (see paragraph 4.7 of our impact assessment guidance[693]).

A2.71 In particular, section 3(4) of the CA 2023 also requires us to have regard to the needs and interests of specific groups of persons when performing our duties, as appear to us to be relevant in the circumstances. These include:

- the vulnerability of children and of others whose circumstances appear to us to put them in need of special protection;
- the needs of persons with disabilities, older persons and persons on low incomes; and
- the different interests of persons in the different parts of the UK, of the different ethnic communities within the UK and of persons living in rural and in urban areas.

A2.72 We examine the potential impact our policy is likely to have on people, depending on their personal circumstances. This also assists us in making sure that we are meeting our principal duty of furthering the interests of citizens and consumers.

Our consultation position

A2.73 In Annex 1 of our December 2023 Part 5 Consultation, we considered whether our proposed guidance would have a particular impact on persons sharing protected characteristics (race, age, disability, sex, sexual orientation, gender reassignment, pregnancy and maternity, marriage and civil partnership and religion or belief in the UK), and in particular whether it may discriminate against such persons or impact on equality of opportunity or good relations. We must also have due regard to the need to promote equality of opportunity and good relations across a range of categories, including those with different political opinions and between those with dependents and those without, as set out in the Northern Ireland Act 1998.

A2.74 Taking account of our general duties under section 3 of the 2003 Act, we considered more broadly whether there were potential impacts on other groups, beyond those that share protected characteristics identified in equalities legislation, such as persons on low incomes.

[692] Ofcom, 2014. Revised Northern Ireland Equality Scheme for Ofcom.
[693] Ofcom, 2023. Impact assessment guidance.

A2.75 The implementation of age assurance using facial estimation alone has the potential to have a greater negative impact on users with the following protected characteristics:

- Age – young adults who are over 18 years old, but who look younger than their age could be negatively affected by false positives that indicate they are under 18 due to being closer to the age threshold;
- Race – some age assurance methods may show varying levels of accuracy against users of different races or with different skin tones; and,
- Disability – users who have a disability which contributes to a visible difference in appearance could be negatively affected if the technology relies solely on facial age estimation that has been trained using a narrow set of example faces.

A2.76 Age assurance methods which rely on the use of ID documents also may have a greater negative impact for users from disadvantaged backgrounds, who are statistically less likely to have a passport or driving licence.

A2.77 We noted that no single method may be completely free of bias and our proposed guidance was designed to help service providers mitigate the potential negative equalities impacts.

A2.78 We set out criteria to assist service providers to implement an age assurance process that is highly effective. This includes the criterion of fairness, which requires the service provider to consider the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes. In addition, we proposed that service providers should consider incorporating the principle of accessibility to ensure that the age assurance process is easy to use and does not unduly prevent adults from accessing legal content due to their characteristics or whether they are members of a certain group.

Summary of responses

A2.79 In relation to Part 5, Sack the Act respondents stated the impact assessment did not discuss the risk of 'outing' members of the lesbian, gay, bisexual, and transgender community when they "verify their identities" on websites.[694]

Our updated impact assessment

A2.80 We have considered consultation responses and have not identified any reason to change our Equality Impact Assessment.

A2.81 As we set out above in paragraph 2.23 of this statement, age assurance solutions must be designed and deployed in compliance with data protection law and follow a data protection by design approach.[695] This includes where age assurance is required by the Act.

A2.82 Specifically, we are not recommending that service providers should undertake identity verification or obtain or retain any specific types of personal data about individual users as part of their highly effective age assurance processes. Our guidance for highly effective age assurance gives service providers flexibility as to the methods they use, rather than specifically recommending they should rely on identity documentation. Further, the UK GDPR requires that service providers, when implementing age assurance methods, collect

[694] Sack the Act responses to our December 2023 Part 5 Consultation, pp.5-6.
[695] ICO, Data protection by design and by default.

the minimum amount of personal data required for the process, and do not retain any personal data collected by the method for longer than is needed. Service providers must not use personal data collected for the purpose of age assurance for any other incompatible purpose.[696] This ameliorates user privacy and security risks potentially posed by age assurance methods, thereby allaying the concerns of the Sack the Act respondents.

Assessing the impact of changes to our final guidance

A2.83 We believe none of the changes to the guidance require any change to our Equality Impact Assessment.

Assessing the impact of our Children's Access Assessments Guidance

A2.84 In this sub-section, we set out our assessment of the likely impact of our guidance for service providers on complying with their duties to carry out children's access assessments, including a summary of our consultation position, and how we have considered responses to our consultation. This impact assessment also captures the impact of our Part 3 HEAA Guidance in the context of Stage 1 of our children's access assessment guidance, which makes reference to highly effective age assurance.[697]

A2.85 The Act itself sets specific duties for providers of Part 3 services to carry out suitable and sufficient children's access assessments and defines relevant concepts such as "likely to be accessed by children" and "the child user condition" as well as specifying how frequently and in what circumstances these children's access assessments should be carried out. The Act requires us to provide guidance to assist services in complying with their duties. Our assessment focuses on areas where we have exercised discretion in making specific recommendations about the steps providers should take to comply with these duties.

A2.86 As discussed in Section 5 (paragraph 5.10), we have exercised discretion in preparing the guidance in specific areas:

- **Age assurance for children's access assessments**, where our Guidance says that where providers conclude that it is not possible for children to access a service, or a part of it, because they are using age assurance, that age assurance should be "highly effective".
- **Our approach to the child user condition**, where we have provided a non-exhaustive list of indicative factors to consider when assessing both criteria of the child user condition.
- **What constitutes a "significant number" of children**, where the guidance says that a relatively small number or percentage of children could be a significant number depending on the context. "Significant number" does not mean that a

[696] Section 1.3 of the Information Commissioner's Opinion for Age Assurance.
[697] The Part 3 HEAA Guidance will also be relevant to any measures in our codes of practice for Part 3 services that refer to highly effective age assurance, which we do not consider here. Our May 2024 Consultation proposed such measures and included our impact assessment of these; we will confirm our position for these measures separately in our Protection of Children statement in April 2025.

large number of children must be using a service or that children form a substantial proportion of users.

- **How service providers can assess whether they are "of a kind likely to attract a significant number of children"**. We have recommended that providers consider the factors provided in the guidance, and any other relevant factors, to build an understanding of whether their service is likely to attract a significant number of children.

A2.87 We received a number of responses on the above issues and have summarised our assessment of the impact of this guidance on various stakeholder groups below. Our summary in the following subsections focuses on any responses which disagreed with aspects of our impact assessment or otherwise raised specific issues, including in relation to the burden on small and micro businesses.

A2.88 We have not made any material changes to our position since the consultation. We have made a number of clarificatory changes to the final version of the guidance which are set out from paragraph 5.16 of this statement.

Impact on regulated service providers, including small and micro businesses

Our consultation position

A2.89 In our May 2024 Consultation, we set out that most services will conclude that they are likely to be accessed by children. We acknowledged this will result in providers of small, low-risk services incurring costs of conducting a children's risk assessment and taking appropriate steps to comply with the children's safety duties. We considered that this largely results from the Act itself and its intent to mitigate risks to children.

A2.90 We set out that based on our proposals related to the child user condition, most services were likely to conclude that they are likely to be accessed by children, and that carrying out children's access assessments will entail only small or negligible costs in most cases. These costs largely derive from the requirements of the Act. Due to the costs being assessed to be small or negligible based on the evidence set out in our May 2024 Consultation, we considered the costs to be proportionate in the context of harm to children that the Act seeks to mitigate.

A2.91 For providers that already use age assurance on their service, there would be some costs in the first stage of the assessment arising from familiarisation with our guidance on highly effective age assurance and assessing it against the kind of age assurance method used by the service, to determine whether it is highly effective. For any services that use highly effective age assurance to comply with specific requirements in the Act to do so, or as part of implementing recommended Code of Practice measures related to highly effective age assurance,[698] such costs would be incurred anyway. However, in any cases where services use age assurance without this being required by the Act or recommended by our Code of Practice measures, these familiarisation and assessment costs would be additional.

[698] We will publish our final decisions on our Protection of Children Codes in April 2025, including an assessment of the likely impacts.

A2.92 Where providers go on to the second stage of the assessment (to determine whether the child user condition is met), we believed that it would require, at minimum, a staff member who would need to read our Children's Access Assessments Guidance, assess, and record the outcome. We expected that most of these service providers will conclude that their services are likely to be accessed by children. For those services, we estimate that reading our Children's Access Assessments Guidance, carrying out the assessment and recording the outcome would take one day of work or less in most cases.

A2.93 We set out that more significant direct costs may apply in limited cases where services believe they are not likely to be accessed by children and decide, at their discretion, to conduct additional work to establish relevant evidence that demonstrates that the child user condition is not met, in line with our proposed guidance. Such costs may reflect analysis related to the number of children on the service to demonstrate the first part of the child user condition is not met. Service providers may also undertake analysis to build evidence related to the appeal of the service to children, to demonstrate that the second part of the child user condition is not met.

A2.94 In both cases we indicated that the costs may include staff costs and/or external costs (e.g., market research commissioned from specialist third-party providers). These costs could vary greatly depending on the context of the service, including the existing evidence the service holds about its age assurance process, its user base, and its appeal to children. For example, commissioning detailed market research could cost tens of thousands of pounds in some cases. We considered that such costs are likely to scale with size of service to some extent. We expected that some services with a very small user base may be able to demonstrate that the child user condition is not met without having to incur large expenses. We provided some illustrative case studies at Annex 2 of the draft Children's Access Assessments Guidance to help service providers understand what such an assessment might look like.[699]

A2.95 Overall, the costs of a suitable and sufficient assessment, required by the Act, mean that the costs incurred by our approach to the assessment are proportionate to the aims of the Act. Our proposed guidance set a high standard for the evidence services are expected to have to demonstrate they are not likely to be accessed by children. As explained above, we recognised that some services could incur additional costs in trying to demonstrate – at their discretion – that they are not likely to be accessed by children.

A2.96 We considered that our proposed approach – and any direct costs resulting to service providers – was proportionate when weighed against the significant benefits to children from reducing the likelihood that services with potential risks of harm to children conclude, incorrectly, that they are not likely to be accessed by children. We considered that our proposed approach also gave service providers the flexibility to choose whether to invest in building evidence or taking any additional steps (such as implementing highly effective age assurance) which may demonstrate that their services are not likely to be accessed by children. Alternatively, service providers could avoid the associated costs by concluding that they are likely to be accessed by children.

[699] Ofcom, 2023, Annex 2: draft Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services

Summary of responses

A2.97 The majority of respondents did not directly respond to the impact assessment of our Children's Access Assessments Guidance. A limited number of respondents disagreed with aspects of our impact assessment in our draft Children's Access Assessments Guidance.

A2.98 The following respondents raised general concerns that our proposed approach to children's access assessments would be burdensome, particularly for small and micro businesses:

- Ukie said that the requirements will be burdensome for its members, including the start-ups, micro and SMEs. They said that smaller game developers may not be able to comply with the "complex requirements", which can curtail the innovation and diversity of the market.[700]
- Inkbunny said that the approach should account for organisations which do not have a commercial business model.[701]
- The Federation of Small Businesses said that the time to comply with the regulation could disproportionately impact small businesses with only a handful of employees.[702]

A2.99 Two respondents commented more specifically on the meaning of 'significant' number of children and the impacts of the proposed approach. Global Network Initiative said that the broad definition of 'significant' number of children would put undue burden on smaller or not for profit services.[703] The Advertising Association said that our interpretation of a 'significant number of children' would put a "compliance burden on services not primarily aimed at children", and place prohibitive costs on new start-up services.[704]

A2.100 Several respondents made comments related to highly effective age assurance, which the Children's Access Assessment guidance refers to as the basis for demonstrating that a service or a part of the service cannot normally be accessed by children (Stage 1 of our guidance). We summarise these responses in the following paragraphs.

A2.101 DuckDuckGo said that our proposed approach means that certain services may have to choose between offering a child-friendly version for all users or collecting and processing the personal data of users through age assurance. They characterised both these outcomes as being disproportionate. [✂].[705] Skyscanner and Mobile Games Intelligence Forum were concerned that implementing highly effective age assurance would create friction in the user experience.[706] One respondent said that the user friction of age assurance will lead to an increase in users leaving the service rather than completing age assurance, which will result in a loss of revenue. They said that the loss of revenue could be substantial, and particularly disproportionate for fundamentally negligible/low risk firms.[707] The Online

[700] Ukie response to our May 2024 Consultation, p.8.
[701] Inkbunny response to our May 2024 Consultation, p.2.
[702] Federation of Small Businesses response to our May 2024 Consultation, p.3.
[703] Global Network Initiative response to our May 2024 Consultation, p.3.
[704] Advertising Association response to our May 2024 Consultation, p.3.
[705] DuckDuckGo response to our May 2024 Consultation, p.3.
[706] Mobile Games Intelligence Forum response to our May 2024 Consultation, p.2; Skyscanner response to our May 2024 Consultation, p.3.
[707] [✂]

Dating and Discovery Association said that our proposed approach could mean some smaller service providers stop trading.[708]

A2.102 Yoti said that service providers which rely on providers of third-party age assurance services may not incur significant costs to demonstrate their approach meets the criteria for highly effective age assurance since providers of third-party age assurance services typically have readily available documentation on the performance of their solutions.[709]

A2.103 Online Dating and Discovery Association called for Ofcom to align with ICO guidance which states that they do not expect services to "implement age assurance methods that: are not currently technically feasible; pose a significant and disproportionate economic impact on businesses; or pose risks to the rights and freedoms of people that are disproportionate to the other processing activities on the service".[710]

Our updated impact assessment

A2.104 We have considered consultation responses and have concluded that our assessment of impacts on service providers broadly still applies. We clarify some aspects of our assessment below, in response to specific stakeholder responses.

A2.105 In response to general comments from stakeholders on the costs of following our Children's Access Assessments Guidance (as set out in paragraph A2.98), we note that all Part 3 services are required by the Act to carry out children's access assessments and the costs that arise from this exercise, as well as the consequences that follow if services are 'likely to be accessed by children' as a result follow from the requirements of the Act. We therefore have not sought to assess these direct impacts. We designed the children's access assessment process with this in mind, aiming to make it a straightforward exercise for most services. We maintain that costs of carrying out the assessment itself are likely to be small or negligible, except in cases where services intend to demonstrate that they are not likely to be accessed by children and need to gather evidence or take additional steps to support this conclusion, as part of a suitable and sufficient children's access assessment. We remain of the view that the process we proposed ensures costs are proportionate, including for small and micro businesses. Our case studies at Annex 2 of the Children's Access Assessments Guidance also illustrate that some services with a very small user base may be able to demonstrate that the child user condition is not met without having to incur large expenses.

A2.106 In response to stakeholder comments about the implications of implementing age assurance, including its cost and the processing of personal data, we note that our Children's Access Assessments Guidance does not recommend that service providers adopt highly effective age assurance. Any service provider who implements highly effective age assurance for the purpose of demonstrating that its service or a part of the service cannot normally be accessed by children (Stage 1 of our guidance) chooses to do so at its own commercial discretion. In such cases, our criteria-based approach in the Part 3 HEAA guidance gives service providers flexibility to adopt a highly effective age assurance process that best suits their needs and to pursue cost-effective approaches, as long as the relevant

[708] Online Dating and Discovery Association response to our May 2024 Consultation, pp.2-3.
[709] Yoti response to our May 2024 Consultation, p.8.
[710] Online Dating and Discovery Association response to our May 2024 Consultation, p.3.

criteria are met. Our assessment is that age assurance which is not highly effective could entail a material risk that children *are* normally able to access the service or part of the service and therefore not protected from harm.

A2.107 We have considered the views of respondents who were concerned that our approach meant services would either need to offer a child-friendly version of the service to all users or collect and process data for age assurance. We acknowledge that this could cause some services to lose revenue or even leave the UK market. We have considered these views and are of the view that this risk is predominantly derived from the Act rather than by exercise of our discretion. This is because the Act requires that where children are normally able to access services (because no highly effective age assurance is in place) and the child user condition is met, such services must comply with the children's risk assessment and children's safety duties, with the effect that the service is a child-friendly version of the service. As such, the Act has the consequence of added friction where highly effective age assurance is implemented or where there are alterations to the service to comply with the children's safety duties. Should services wish to continue to operate in the UK market, they are required to comply with this legal framework and potential costs to the service are a consequence of the Act rather than due to the exercise of Ofcom's discretion. This outcome is proportionate to the Act's aim to ensure a safer online experience for children, and a higher level of protection than for adult users.

A2.108 In response to Online Dating and Discovery Association's comments, our Part 3 HEAA Guidance gives service providers flexibility in adopting the age assurance process that best suits their needs, which includes selecting methods which are technically feasible for them or are otherwise preferable for their specific context, subject to meeting the expectations set out in the Guidance.

Rights assessment

A2.109 Further to consideration of stakeholder responses to consultation, we have not changed our rights assessment for the Children's Access Assessment Guidance. This derives from the children's access assessment being evaluative rather than requiring any positive action by service providers that could infringe upon user rights. Ofcom's interpretation of the child user condition, particularly the "significant number" element of both parts of the child user condition is likely to mean that most services find that children are likely to access their service within the meaning of the Act. This is largely a consequence of the Act itself, which seeks to ensure that where children are likely to access services, their experience will be child-friendly. Where services conclude that they are not likely to be accessed by children due to the use of highly effective age assurance, this may build in friction for adult users who are required to verify that they are not children. In our view, this friction is proportionate to the aims of the Act, including that children be provided a higher level of protection that adults. As such, our conclusion is that our approach to the children's access assessment set out in our Guidance is proportionate to the aims of the Act.

A2.110 In Annex 1 we have set out Ofcom's duties under the ECHR.[711] In carrying out our rights assessments under the Children's Access Assessments Guidance, we have addressed the relevant rights impacts on users, services and other persons and have considered the extent to which our proposals may interfere with certain rights in the ECHR as set out in Schedule 1 of the Human Rights Act 1998. Further detail is set out in Annex 1.

A2.111 The purpose of the guidance is to assist service providers in complying with the duties relating to children's access assessments, which is a statutory requirement, set out in the Act. In developing our approach to this guidance we have, as set out above, exercised some degree of discretion as to how we do this. Our approach to the Children's Access Assessments Guidance means that providers would be asked to consider a number of aspects relating to user access, age assurance and the make-up of a service itself, for example, the types of content hosted and the service design.

A2.112 As noted above, we have considered the impact of our Part 3 HEAA Guidance in the context of Stage 1 of our Children's Access Assessment Guidance, which makes reference to highly effective age assurance. However, we have not taken into account stakeholder comments about the rights impacts associated with our proposed age assurance measures in our draft Protection of Children Code for user-to-user services, in relation to which the Part 3 HEAA Guidance is also relevant. We will address those impacts in April when we reach decisions on the Protection of Children Codes.

Freedom of expression and freedom of association

Summary of responses

A2.113 In response to our consultation position on stage one of the children's access assessment, Big Brother Watch opposed the fact that services could only rule themselves out scope of the children's safety duties if they had highly effective age assurance, as they suggested that this forces services to implement age assurance or content moderation tools which would have adverse impacts on individuals' rights to both free expression and privacy.[712] Some respondents suggested that services might choose to use highly effective age assurance to block children altogether rather than creating child safe experiences.[713] Integrity Institute argued that "age assurance overall provides a poor grounding and foundation for child safety."[714] The Advertising Association and Global Network Initiative also highlighted that the children's access assessment means that it is likely that many services may choose to adopt highly effective age assurance.[715] Some respondents were concerned that implementing highly effective age assurance may create friction in the user experience.[716]

[711] Human Rights Act 1998 c.42.
[712] Big Brother Watch response to our May 2024 Consultation, p.2.
[713] Big Brother Watch response to our May 2024 Consultation, p.3; Global Network Initiative response to our May 2024 Consultation, p.4; Samaritans response to our May 2024 Consultation, p.4.
[714] Integrity Institute response to our May 2024 Consultation, p.2.
[715] Advertising Association response to our May 2024 Consultation, p.3; Global Network Initiative response to our May 2024 Consultation, p.4.
[716] Mobile Games Intelligence Forum response to our May 2024 consultation, p.2; Skyscanner response to our May 2024 consultation, p.3; Mid Size Platform Group response to our May 2024 Consultation, p.3.

A2.114 DuckDuckGo suggested that the approach means that certain services may have to choose between offering a child-friendly version for all users or collecting and processing the personal data of users through age assurance. They characterised both these outcomes as being disproportionate. [✂]. Free Dating Limited highlight that the high user dop-off rate associated with HEAA may make businesses unviable.[717]

A2.115 As noted at paragraph [5.126], some respondents suggested that services might choose to use highly effective age assurance to block children altogether rather than creating child safe experiences. The NSPCC suggested this could have "significant, negative implications for children's rights to access the online world and make use of digital services".[718]

Our final rights assessment

A2.116 We consider that our guidance would not disproportionately interfere with users' (including children and adults) rights to freedom of expression or association.

A2.117 Our approach to children's access assessments recommends that service providers assess their service(s), or a part of the service, and determine whether it is possible for children to access it and whether one or both limbs of the child user condition are met, in line with the requirements of the Act. It does not require or recommend that services make any changes to their services or implement technologies that are not already in place, such as implementing highly effective age assurance.

A2.118 While some services may take a commercial decision to implement highly effective age assurance to avoid the need to implement the child safety duties, they will nonetheless still be subject to illegal content duties which, in some cases, overlap with child safety duties lessening the ability (and therefore, the incentive) to avoid duties under the online safety regime by implementing highly effective age assurance. As such, we consider widespread implementation of highly effective age assurance purely for the purpose of avoiding children's duties is unlikely to materialise and as such that the impact to users' rights to freedom of expression and freedom of association is likely to be limited.

A2.119 We have considered respondents' concerns that the impact of either implementing highly effective age assurance or complying with the child-safety duties to create a child-friendly service experience are disproportionate, and that the high user drop off rate may make business unviable and limit the ability of UK users to exercise their rights to freedom of expression and association via these services. The framework by which services must comply with the child safety duties if it is possible for children to access the service and likely that they will do so derives from the Act itself. The Act provides a higher level of protection to children online than adults and therefore the operation of the children's access assessment bringing most services to be in scope of child safety duties is proportionate to that aim.

A2.120 We have taken the decision in the context of the Children's Access Assessment Guidance that age assurance needs to be highly effective in order to conclude it is not possible for children to access the service (or part of it) because it is unlikely that forms of age assurance that are not highly effective at determining if a user is an adult or child would be

[717] Free Dating Limited response to our May 2024 Consultation, p.2.
[718] NSPCC Response to our May 2024 Consultation, p.6.

able to ensure compliance with the Act. As such, our approach is guided by the Act and the intentions underpinning children's access assessments, including that children be given a higher level of protection than adults. We consider the friction and impact to adults' freedom of expression derives from the Act's requirement that services undertake children's access assessments. We consider our approach to the children's access assessment is proportionate to the benefits to children by services either implementing highly effective age assurance or implementing child safety duties.

A2.121 We accept that there will be some friction for adult users using services that implement highly effective age assurance. We consider providers have incentives to make their age assurance process as user-friendly as possible and limit friction to adult users. Alongside this, the public awareness campaigns that Ofcom will run to encourage adults to engage with age assurance rather than visit sites that may be less safe. We also note that users identified as adults via services' age assurance process will be able to use the service, limiting the impact of this upon their freedom of expression and association.

A2.122 In response to comments made by the NSPCC of potential significant, negative implications for children's rights to online access, we acknowledge that if services choose to implement highly effective age assurance to prevent children from accessing the entire Part 3 service (or a part of it), this would have an impact on children's rights to freedom of expression and association, as they would no longer be able to access these services (or the relevant parts of those services). However, we consider that this is an impact that arises from services' commercial decisions (in line with their own rights under Article 10 to control the users they allow to access their services), rather than as a result of Ofcom's approach taken in the Children's Access Assessments Guidance, as we are not recommending that services must use highly effective age assurance. We also consider that it would not be in the best interests of children if services were permitted to implement a form of age assurance for the purposes of stage 1 of the children's access assessment which was not highly effective at correctly determining whether or not users are children. This is because there would be a material risk children would still be able to access the service without benefiting from appropriate protections from harm as required under the children's safety duties in the Act.

A2.123 We consider the impact on providers' and users' freedom of expression to be limited insofar as the measures will not require services to actively alter the design of their service. The factors that we suggest that services have regard to when determining whether they are of a kind likely to attract a significant number of users who are children include particular types of content and the ways in which a service might be appealing or beneficial to children as a result of functionalities or the presentation of a service. In considering whether the child user condition is met, we do not suggest that providers should take any particular steps on content or the design features of a service, rather they are to consider the service as a whole, including data on the number of users if available (and reliable) and determine whether either or both limbs of the child user condition is met. As our approach to the assessment does not recommend a change to services' operation, we do not consider the impact on service providers' freedom of expression to be significant.

Privacy and data protection

A2.124 We refer to the human rights legal framework in regards to privacy in the UK, set out in Annex 1. Below we consider stakeholder concerns about the privacy and data protection impacts of our approach to the children's access assessment.

Summary of responses

A2.125 Privacy concerns of stakeholders in response to the consultation can be summarised as follows:

- Some respondents raised user privacy concerns associated with the implementation of highly effective age assurance.[719] Global Network Initiative suggested taking a more flexible approach to children's access assessments and age assurance until more rights-protecting age assurance methods are available.[720] Some respondents expressed concern about the amount of personal data that would be collected and processed because of providers implementing age assurance.[721] Big Brother Watch and the Integrity Institute warned about the risk of data leaks generally.[722]
- Some stakeholders expressed concern about the privacy and data protection impact of children's access assessments. Northeastern University London and Wikimedia were concerned that carrying out children's access assessments would lead to services intrusively monitoring and tracking users.[723]

Our updated rights assessment

A2.126 We consider that our guidance would not disproportionately interfere with users' (including children and adults) rights to privacy. As noted above, we have exercised our regulatory discretion to set out that, where a provider seeks to conclude that children are not normally able to access a service or a part of it, any age assurance which is being used

---

[719] Skyscanner response to our May 2024 Consultation, p.3; DuckDuckGo response to our May 2024 Consultation, pp.2-3; Global Network Initiative response to our May 2024 Consultation, pp.4-5.
[720] Global Network Initiative response to our May 2024 Consultation, p.5.
[721] [✂]; Association of Police and Crime Commissioners response to our May 2024 Consultation, p.3; Big Brother Watch response to our May 2024 Consultation, pp.22-23; Burville, M response to our December 2023 Part 5 Consultation, pp.1-3; Collier D, response to our December 2023 Part 5 Consultation, pp.1-3; Free Speech Coalition response to December 2023 Part 5 Consultation, p.7; ; Fringe Dweller Productions response to our December 2023 Part 5 Consultation, pp.1-3; Global Network Initiative response to our May 2024 Consultation, pp.4-5; Mega Limited response to our May 2024 Consultation, p.14; Hutchison, A response to our December 2023 Part 5 Consultation, p 2-3; Jackson, EM response to our December 2023 Part 5 Consultation, p 2-3; ID Crypt Global response to December 2023 Part 5 Consultation, p.1; Name withheld 9 response to our December 2023 Part 5 Consultation, p.3; Mid Size Platform Group response to our May 2024 Consultation, p.3; Pinterest response to our May 2024 Consultation, p.12; Integrity Institute response to our May 2024 Consultation, pp.2-3; Northern Ireland Commissioner for Children and Young People (NICCY) response to May 2024 Consultation, p.31; Name Withheld 8 response to our December 2023 Part 5 Consultation, pp.2-3; Name Withheld 1 response to our December 2023 Part 5 Consultation, pp. 1-3; Name Withheld 2 response to our December 2023 Part 5 Consultation, pp.2-3; Name Withheld 3 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 4 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 5 response to our December 2023 Part 5 Consultation, pp.1-3; Name Withheld 6 response to our December 2023 Part 5 Consultation, pp.1-3; Safazadeh, S, response to our December 2023 Part 5 Consultation, pp.1-3; Shaw, A. response to our December 2023 Part 5 Consultation, pp.1-3; Warren A, response to our December 2023 Part 5 Consultation, pp.2-4; xHamster response to our December 2023 Part 5 Consultation, p.3; xHamster response to our May 2024 Consultation, p.2; 14 further confidential individual respondents to our December 2023 Part 5 Consultation, pp.1-4.
[722] Big Brother Watch response to our May 2024 Consultation, p.22; Integrity Institute response to our May 2024 Consultation, p.2.
[723] Northeastern University London response to our May 2024 Consultation, p.8; Wikimedia response to our May 2024 Consultation, p.3.

to achieve that result should be highly effective at correctly determining whether a particular user is a child. Ofcom's proposed approach to the child access assessment, however, did not recommend services should specifically implement age assurance measures, nor recommend they process or retain any specific kinds of personal data which they would not already have available to them to carry out the children's access assessment, though it may entail the processing of existing data available to them for new purposes. This could be done in a data minimising way, i.e. not recording any more detail of the user than is necessary and only based upon the data that services already collect.

A2.127 As we stated in our consultation, we consider that the only services likely to have sufficiently accurate data on the age of their users for this purpose would be those using highly effective age assurance. The ICO's opinion on age assurance in its Children's code[724] is clear that it is both possible and a legal requirement to operate age assurance in a privacy-preserving way. We address this in the 'Privacy, data protection and security concerns with highly effective age assurance' section of this Statement from paragraph 3.262. Built into the children's access assessment is the requirement that services consider whether it is possible for children to access their service (or part of it). Our approach is that services are only able to conclude that it is not possible for children to access their service where they are using highly effective age assurance. Processing of user data is not required for services to identify whether or not their service currently implements highly effective age assurance.

A2.128 Our approach to the child user condition does not recommend the processing of personal data. In relation to the child user condition, we exercise our regulatory discretion to set out what we consider to be relevant factors which providers should consider when assessing whether a service has a significant number of children who are users of the service, or whether the service is of a kind likely to attract a significant number of users who are children. The factors we set out within the guidance are broad in scope reflecting the diversity of services in scope of the Act and evidence on children's online habits.

A2.129 We acknowledge that if all Part 3 services who do not currently implement highly effective age assurance sought to track and monitor user data to form a view as to how many users of their service are likely to be children, this would lead to widespread and significant processing of users' personal data. This is not what we are recommending in the Children's Access Assessment Guidance, and instead we have set out a list of factors for services to consider when assessing whether their service is likely to meet the child user condition, including whether a significant number of their users are children. We have adopted an approach that is more context-specific rather than using a numerical threshold to assist services in taking a more holistic approach to considering the nature of their service and to reflect the diverse range of services undertaking this assessment. This approach does not recommend or require the processing of new or existing user data to reach a decision as to whether the child user condition is met. Our approach also does not recommend the profiling of users, such as through age inference technologies. We remind respondents who have expressed concerns about the use of the term "significant number" that while Ofcom has discretion to explain a 'significant number of users who are children' within the context of the child user condition, the 'significant number' concept derives from the Act

[724] ICO, 2024, Age Assurance for the Children's Codes.[accessed 22 December 2024].

and therefore must apply. As such, the possibility of services choosing to process users' personal data to calculate the number of child users they have would exist no matter how Ofcom uses its discretion to explain 'significant number'.

A2.130 We consider that our approach to implementing highly effective age assurance may help to safeguard users' rights to privacy as it should help to limit the risk of incorrect assessments of age due to ineffective age assurance methods, provided that services take account of our recommended approach set out in the Part 3 HEAA Guidance. In addition, we are clear that any processing of personal data for the purposes of implementing highly effective age assurance, or otherwise for the purposes of carrying out the children's access assessment, would need to be carried out in accordance with data protection legislation.

Welsh Language Impact Assessment

A2.131 We refer to the legal framework regarding the Welsh language in A2.58 above where we set out Ofcom's duties under The Welsh Language (Wales) Measure 2011 to comply with certain Standards in relation to the Welsh language.

Our consultation position

A2.132 The Act specifies that services must keep a written record of their children's access assessment.[725] In our draft Children's Access Assessments Guidance we proposed that services can choose to keep written records in English or, for service providers based in Wales, in English or Welsh.

Summary of responses

A2.133 We did not receive any stakeholder pushback or alternative recommendations in relation to our Welsh Language Impact Assessment for the children's access assessment.

Our updated impact assessment

A2.134 Further to consideration of stakeholder responses, we have not identified any reason to change our Welsh Language Impact Assessment and will be maintaining the position set out at consultation that services can choose to keep written records in English or, for service providers based in Wales, in English or Welsh.

Equality Impact Assessment

A2.135 In A2.66 above we have set out Ofcom's duties under the EA 2010 and the Northern Ireland Act 1998.

A2.136 In relation to children's access assessments, we consider that the Guidance should help to secure a higher level of protection to children, by helping service providers understand how to comply with their duties to carry out suitable and sufficient children's access assessments. This in turn will contribute to mitigating against the risk that Part 3 services which are likely to be accessed by children wrongly conclude that they are not likely to be accessed by children and therefore do not comply with the duties in the Act to carry out children's risk assessments and takes steps to protect children from harm. This ensures

[725] Section 36(7) of the Act.

that children using regulated services will have a safer online experience by being subject to the safeguards and support of the children's safety duties.

A2.137 Our approach in the Children's Access Assessments Guidance sets out that services are only able to conclude that it is not possible for children to access a service where they have highly effective age assurance in place. In setting this approach, we have considered the potential discriminatory impacts and biases built into some age assurance technologies and processes. We have addressed this risk in our consideration of the equality impacts of our approach to Part 5 at A2.75 above. We do not recommend or encourage the processing of user data to infer users' age and thereby does not build in the potential for bias and incorrect judgments by use of age inference technologies. We instead encourage that services undertake a holistic consideration of their service to determine whether the child user condition is met, without profiling users on that service.

A3. Children's access assessments: sources of evidence

A3.1 This annex sets out the evidence we drew on in formulating the list of factors for service providers to consider when determining whether the child user condition is met as part of a children's access assessment (Children's Access Assessments Guidance, Section 4, Tables 6 and 7).

A3.2 The methodology underpinning the development of this list of factors in Section 4 of the Children's Access Assessments Guidance consisted of desk research to collate literature on the topic of children's interests online and research developed and published by Ofcom.

A3.3 We originally set out this evidence at Section 5 of our May 2024 Consultation. We have updated sources where more recent evidence is now available. We have not made any other changes to our summary of evidence in response to stakeholder feedback.

Children are exposed to, and many seek out, an adult experience online

A3.4 Increasingly, social media is where children go to learn about the world.[726] Some children say they spend a huge amount of time on consuming large quantities of online content.[727] They use online spaces for activities across all areas of their lives – including friendship, connection, education and engaging with culture.[728] The internet has become part of "youth culture".[729]

A3.5 Our research suggests many children are using online services before the minimum age specified by services, with a significant minority seeking an even older experience online. For example, 51% of children under 13 told us that they have used social media or apps before the minimum age.[730] Just over a third (36%) of 8-15s, with a social media profile, have a user/profile age of at least 16 and just over a fifth (22%) of 8–17s have an adult profile (18+).[731]

A3.6 The ICO and LSE's report on Children's data and privacy online reflects that when children do not agree with age limits, they find a way to bypass the limits, for example by entering a different age. This research indicated that children proactively engage with content that is not specifically designed for children. Children tend to view age-appropriate labelling as "rough guidance", underpinning the conclusion that children may seek an adult experience

[726] Ofcom, 2024. Children and Parents: Media Use and Attitudes.
[727] Ofcom, 2022. Research into risk factors that may lead children to harm online.
[728] Ofcom, 2022. Research into risk factors that may lead children to harm online.
[729] mediasmarts.ca. How Marketers Target Kids. [accessed 1 February 2024].
[730] Ofcom, 2024. Children and Parents: Media Use and Attitudes.
[731] Ofcom, 2024. Children's Online User Ages 2024 (Wave 3). Quantitative Research Study.

online, proactively engaging with content that is flagged as not appropriate for their age online.[732]

A3.7 In its response to our 2023 Protection of Children Call for Evidence ("2023 CFE"), 5Rights flagged that "children do not only use services explicitly targeted or designed for them",[733] while UK Safer Internet Centre (UKSIC) noted that "there is a desire to push age restriction boundaries".[734] This reflects that children, likely older children, may seek an adult experience online. Evidence clearly suggests that children are seeking an adult experience online and are attracted to age-restricted services. For example:

- Pornography services are a key space children explore online. Some children who participated in a small sample study which we conducted told us that they were being served content of a sexual nature by platforms.[735] Other research suggests many young people seek out pornography online (including via search services) while others encounter this unintentionally.[736] [737] The average age at which children say they first see pornography is just 13 years old.[738]
- In its response to our 2023 CFE, the Online Dating Association stated that, "In relation to the online dating space, children can sometimes be attracted to dating services which are aimed at adults with whom they are close in age. Within the dating sector, we find children who are interested in dating platforms tend to fall in the 15–17 year old age range".[739]

A3.8 While there is huge variation by age in the way children engage online, evidence suggests that children want to engage with services not specifically targeted at them.[740] [741] [742] The

[732] London: London School of Economics and Political Science, (Stoilova, M., Livingstone, S. and Nandagiri, R.), 2019. Children's data and privacy online: Growing up in a digital age. Research findings. [accessed 30 January 2024]
[733] 5Rights response to 2023 Protection of Children Call for Evidence.
[734] UK Safer Internet Centre (UKSIC) response to 2023 Protection of Children Call for Evidence.
[735] Ofcom, 2022. Children's Media Lives. Subsequent references to the report throughout.
[736] Results from a survey conducted by the Children's Commissioner indicated that 30% of children had reported seeing pornography on "search engines". Children's Commissioner, 2023. A Lot of it is Actually Just Abuse – Young People and Pornography. [accessed 9 January 2025] Subsequent references to the report throughout.
[737] In research with UK children many respondents described their first viewing of pornography as "accidental", including through "Google searches where many described unwittingly searching terms such as 'sex' or 'porn' without understanding what these words meant"; BBFC, 2020. Young People, Pornography & Age-verification.
[738] Children's Commissioner, 2023. A Lot of it is Actually Just Abuse – Young People and Pornography.
[739] Online Dating Association's response to 2023 Protection of Children Call for Evidence.
[740] Ofcom, 2023. Children and Parents: Media Use and Attitudes.
[741] See London: London School of Economics and Political Science (Stoilova, M., Livingstone, S. and Nandagiri, R.), 2019. Children's data and privacy online: Growing up in a digital age. [accessed 22 April 2024]; Research findings; ICO, 2019. Towards a better digital future Informing the Age Appropriate Design Code. [accessed 22 April 2024]
[742] Ofcom, 2023. Online Nation 2023. Subsequent references to the report throughout. Ofcom's Children's Online Passive Measurement Pilot study showed that Roblox was the only organisation in the top five reaching organisations by UK online children aged 8-12 that did not appear in the top five for those aged 15+. Note: Pilot study data is not weighted. Due to low base size (162) data should be treated as indicative only and not representative.

available evidence suggests that children, especially older teenagers, use a wide range of online services in a way that is similar to adults.[743]

A3.9 A comparative example may be taken from streaming services. Our research demonstrates that children's favourite shows on Netflix were adult-geared shows: such as *Squid Game* (rated 15) and *You* (rated 18). This is reflective of a theme throughout the evidence that children are being exposed to, and in some cases seeking, an adult experience online.[744] Industry viewing data from Barb also shows this. Some of the most watched programmes by those aged 13 – 17 were aimed at older children/adults – including *Squid Game*, *Black Lightning* (rated 15), and *The Sidemen Story* film (rated 15). The most-watched programmes among the 4-17 age group included the 18-rated comedy series *Beef*.[745]

A3.10 Ofcom research and that of the Office for National Statistics found that the most common activities for children online included social media, messaging and gaming and watching videos online, among other activities.[746] Evidence from the Children's Commissioner for England's report into social media use among 8–12-year-olds found that younger children used a parent's phone to access social media services. This meant they were able to access Facebook and Twitter.[747]

A3.11 While evidence indicates that children today are less likely to use search services as frequently, or in the same way, as adults, the vast majority of children still use search services in some capacity.[748] [749] There is some published research on the topic of children's access to pornographic content via search services, including quantitative research in which children report seeing pornography on or via search services.[750] Search services are also mentioned in qualitative research as one of the ways that children first encountered pornographic content, both intentionally and unintentionally.[751]

---

[743] See Ofcom, 2023. Online Nation 2023.
[744] Ofcom, 2022. Children's Media Lives.
[745] Barb as viewed. Ranked by the total audience for a title's best performing episode, across October 2023 – March 2024.
[746] ONS, 2020. Children's online behaviour in England and Wales: year ending March 2020 [accessed 30 January 2024]; Ofcom, 2024. Children and Parents: Media Use and Attitudes. Subsequent references to the report throughout.
[747] Children's Commissioner, 2018. Life in 'likes' Children's Commissioner report into social media use among 8-12 year olds. [accessed 30 January 2024]. Subsequent references to the report throughout.
[748] Google executives have talked publicly about the changing nature of search activity conducted by children (see: Perez, S, 2022. Google exec suggests Instagram and TikTok are eating into Google's core products, Search and Maps, techcrunch.com, 12 July 2022) [accessed 30 January 2024]; while a raft of research with children, including Ofcom's Children's Media Lives 2023 report shows how children conduct their online searching on a wide range of platforms, often starting with social media or video-sharing platforms.
[749] More than nine in ten (95%) children aged 8-17 in Ofcom's 2024 children and parents' media use and attitudes research claimed to use search engines. Ofcom, 2024. Children and Parents: Media Use and Attitudes.
[750] Results from a survey conducted by the Children's Commissioner indicated that 30% of children had reported seeing pornography on "search engines". Children's Commissioner, 2023. A Lot of it is Actually Just Abuse – Young People and Pornography.
[751] In research with UK children many respondents described their first viewing of pornography as "accidental", including through "Google searches where many described unwittingly searching terms such as 'sex' or 'porn' without understanding what these words meant". BBFC, 2020. Young People, Pornography & Age-verification.

A3.12 Other examples highlight the role search services play alongside social media in enabling children to encounter pornographic content.[752]

A3.13 Taken together these insights suggest that children are not deterred by age restrictions or from services targeted at older age groups and many are likely to be encountering content (and harms online) in a similar way to adults.

A3.14 We discussed a range of other evidence suggesting that children encounter harmful content online in Volume 3 of our May 2024 Consultation, which incorporated our draft Children's Register of Risks and Guidance on Content Harmful to Children. We will publish final versions of these products with our April Protection of Children Statement.

List of factors

A3.15 Below we set out the evidence and rationale in support of the list of factors in Section 4 of the Children's Access Assessments Guidance that service providers should consider when carrying out their assessment of whether the child condition is met.

The service provides benefits for children

A3.16 Evidence demonstrates that a service which benefits children is likely to attract children. Children benefit from being online as it helps them with various activities. Children go online for lots of different reasons. In our research, children's responses to "Being online helps me with…" included:

- Schoolwork/homework
- To build or maintain friendships
- To find useful info about personal issues
- To learn a new skill
- To find out about the news
- To develop creative skills
- To understand what other people think and feel
- To develop skills with reading and numbers
- To find out more about, or to support causes.[753]

A3.17 We have included whether the service benefits children as a factor in the Children's Access Assessment Guidance because it is a useful starting point for a provider to consider whether their service is of a kind likely to attract children. This is because children are likely to be attracted to services that offer some benefit to them. For example, if a service provides the benefit of entertainment or the chance to connect and build relationships, it is likely that children will be attracted to such a service. Providers should take a holistic

[752] Ofcom research from 2022 provides one example: Ethan (10 years old) reported coming across porn after searching a term [the name of a lesser-known porn site] after seeing a video on a social media platform about it. The post read "don't ever search [name of porn site] up" that enticed Ethan to see what it was. "I saw this [video], and it said, 'Don't ever search this up'. I searched it up [using a search engine] as I thought it was just going to be a little scary thing or whatever… They were right [I shouldn't have searched the term]." Ofcom, 2022. Risk factors that may lead children to harm online.

[753] Ofcom, 2024. Children and Parents: Media Use and Attitudes.

approach when considering whether their service may provide benefits to children of any age.

The content on a service appeals to children

A3.18 Some content types are particularly likely to attract children. The content published on a service may contribute to making the service useful and enjoyable for children.

A3.19 Ofcom's research points to a range of content consumed by children on video sharing platforms – including funny videos, educational and tutorial content, and sports highlights and clips.[754] An Ofcom pilot study that passively measured internet use of 162 UK 8–12 year olds online found almost all of the children visited a social media service (97%).[755] A growing proportion of this content is consumed in short-form video presented through recommender systems, which use algorithms to tailor content to each user. Platforms such as TikTok and YouTube Shorts offer children convenience and personalisation in their online experience – factors that are increasingly common to the way that they consume content.[756]

A3.20 We have included this factor in the Children's Access Assessment Guidance because if a service hosts or publishes content that is appealing to children, it strongly indicates that the service will meet the child user condition. A provider will benefit from reviewing the list of content types and considering whether their service hosts or publishes any other type of content that may be appealing to children.

A3.21 We have provided evidence in Table 5.1 below to demonstrate the relevance of these particular content types.

[754] Ofcom, 2018; Research into children's content consumption, including Netflix and YouTube;. Children and parents: media use and attitudes report 2024 – interactive data.
[755] Ofcom Ipsos Children's Passive Measurement Pilot 2023, age: 8-12, UK. Base: 162. Data is not weighted. Due to low base size data should be treated as indicative only and not representative. Cited in Ofcom, 2023. Online Nation.
[756] Ofcom, 2022. Children's Media Lives.

Table A3.1: Indicative examples of content types that are appealing to children

Content type	Evidence
Entertainment and popular culture	Film, music, television, comedic, cartoons, animation, fashion and content by and about influencers and celebrities. Four in ten children aged 3-17 are consuming content from influencers.[757] Children are interested in entertainment and content related to popular shows. Our own research demonstrates that children's favourite shows on Netflix were adult-geared shows: Squid Game (rated 15) and You (rated 18) for example.[758]
Creative activities	A GCHQ/DCMS report found that fundamental online experiences for children include "creating and consuming content".[759] Evidence suggests that children use the internet to upload content, for example five in ten girls between 12–17 had posted videos on VSPs. Four in ten boys had posted videos on VSPs.[760]
Games and sports	Nearly six in ten (57%) children between 3–17 play video games online.[761] Online gaming is one of the central experiences of children online.[762] Sport content is also an area of interest for children.[763]

[757] Ofcom, 2022. Children and parents: media use and attitudes report 2022; Ofcom, 2023. Children and Parents: Media Use and Attitudes; Ofcom, 2023. News Consumption in the UK. Subsequent references to the report throughout.
[758] Ofcom, 2022. Children's Media Lives.
[759] GCHQ, DCMS, 2020. The Verification of Children Online: Phase 2 Report. [accessed 30 January 2024]. Subsequent references to the report throughout.
[760] Ofcom, 2024. Children and Parents: Media Use and Attitudes 2024.
[761] Ofcom, 2024. Children and Parents: Media Use and Attitudes 2024.
[762] GCHQ, DCMS, 2020. The Verification of Children Online: Phase 2 Report.
[763] Catch 22 response to 2023 Protection of Children Call for Evidence.

Content type	Evidence
Making connections, friendships, dating and relationships	Evidence suggests that children are interested in similar topics to adults, including relationships, sex, and dating.[764] In their response to our 2023 CFE, the Online Dating Association noted that "children can sometimes be attracted to dating services which are aimed at adults with whom they are close in age. Within the dating sector, we find children who are interested in dating platforms tend to fall in the 15–17-year-old age range. This means that for many, their close-in-age peers who are 18+, who they may know from community groups, school or sports, are allowed to use dating services. This could make it tempting for those within this age group".[765] Children use their time online to build and develop relationships with those around them. A UKCCIS report into children's online activities noted that, for children between the ages of 7–16, communicating with friends and family was one of the most popular reasons for going online and becomes more popular as children get older.[766]
Self-improvement, lifestyle, and careers	Online content can be a way for children to learn more about their own interests: many follow accounts and view content that enables them to learn skills that they perceive as useful either at present or for their future career.[767] Some children will use this inspiration to engage in their own content creation, including making videos, editing photos, or creating art to share with others.[768] The rise in the prominence and popularity of influencers has affected children's own aspirations. A growing number of 8–12 years olds express a desire to pursue this as a career path later in life; some view the figures they follow and watch online as inspirations and use their content as a drive for their own ambitions.[769]

[764] BBFC, 2019. Children see pornography as young as seven, new report finds; Common Sense Media, 2023. Common Sense Media's response to 2023 Protection of Children Call for Evidence.
[765] Online Dating Association, 2023. Online Dating Association response to our 2023 CFE.
[766] UKCCIS, 2017. Children's online activities, risks and safety. [accessed 31 January 2024]. Subsequent references to the report throughout.
[767] Children's Commissioner, 2018. Life in 'likes' Children's Commissioner report into social media use among 8-12 year olds.
[768] The Insights Family, proportion of children aged 3–17 who agree that 'I like learning new things' is certainly or somewhat true. Cited in Ofcom, 2023. Children and Parents: Media Use and Attitudes.
[769] Children's Commissioner, 2018. Life in 'likes' Children's Commissioner report into social media use among 8-12 year olds.

Content type	Evidence
Health, challenges, and support	Our research suggests that children use different resources to manage their wellbeing online, using different services to find out about topics like healthy eating, puberty, exercise, health symptoms, and meditation.[770] They are also likely to turn to content produced by others to support them, including influencers and services focusing on fitness and wellbeing.[771]
Education, learning and knowledge	Children often use online resources to support them in their own education, including studying, homework, and to look up information on subjects that interest them. Examples include online resources that support mathematics like Times Tables Rockstars and language learning like Duolingo are used among online children aged 8–12. Older children are also interested in language learning apps like Duolingo, and access publicly available information sources like Wikipedia and U2U educational forums like Quora and The Student Room.[772]
Current affairs and engaging in social activity	Ofcom's indicative research into news consumption among 12–15-year-olds suggests that children commonly use Part 3 services including TikTok, Instagram, and YouTube as an important source of information on current affairs rather than traditional broadcasters and publishers.[773]

A3.22 Service providers should note that, as discussed above at A3.7, evidence shows that children are also attracted to content that is intended for adults, including pornography.

The design of a service appeals to children

A3.23 Evidence suggests that the design of a service may also play a role in attracting children to a service. This includes colour and presentation in addition to the features and functionalities on a service. In terms of colour and presentation, responses to our 2023 CFE reflect the importance of colour, cartoons, animations, diagrams, graphics, exciting narratives and other interactive features.[774] Our research suggests that children engage

[770] Ofcom, Online Research Panel Poll: Children's wellbeing online, August 2023. See Online Nation 2023 Report.
[771] Ofcom, 2024. Children and Parents: Media Use and Attitudes.
[772] Ofcom Ipsos Children's Passive Measurement Pilot 2023, age: 8–12, UK / Ipsos, Ipsos iris Online Audience Measurement Service, Ranking report, Category: Education, May 2023, age: 15–17, UK. Cited in Ofcom, 2023. Online Nation 2023 Report.
[773] Ofcom, 2023. News Consumption in the UK.
[774] ICO response to 2023 Protection of Children Call for Evidence; National Center for Missing and Exploited Children response to 2023 Protection of Children Call for Evidence; ParentZone response to 2023 Protection of Children Call for Evidence.

with and utilise a range of features and functionalities including messaging, video watching via streaming and user-created videos, and downloading content.[775]

A3.24 Children use functionalities to connect with others. They use their time online to build and develop relationships with those around them. UKCCIS's report into children's online activities noted that, for children between the ages of 7 and 16, communicating with friends and family was one of the most popular reasons for going online and becomes more popular as children get older.[776] If a service has features and functionalities that make it possible for children to create and upload their own content, this service is likely to appeal to children seeking to express themselves online and be creative, as uploading content they have created themselves allows others to see it.[777]

A3.25 Our research also shows that Part 3 services, and the functions within them that children use to interact with other children, appear to be increasingly distinct from those used to consume and create content. 'Feeds' are for content, 'chat' is for social interaction.[778]

A3.26 We have included this factor because it is important for a provider to consider how the appearance of their service may attract children. It is also important for a provider to consider whether the way the service is designed, the functionalities and features, increase the likelihood of children using and enjoying the service.

Children are part of a service's commercial strategy

A3.27 In the Children's Access Assessment Guidance we have encouraged providers to consider various factors related to their commercial strategy. These factors include whether children form part of the provider's marketing strategy for its service; whether the provider allows advertising, promotions or competitions targeted at children on their service; whether the nature, design, or content of the adverts on the service are appealing to children; whether children form part of the service's growth strategy; and the commercial profile of the service. We have included these factors because they help a provider understand whether their service is proactively targeting children or indirectly targeting children.

A3.28 Other factors related to providers' commercial strategies include services' revenue streams and sources of turnover, as well as other information captured in management accounts or annual reports, which may suggest that children are an audience for a service.[779]

A3.29 Evidence suggests that advertising on the service and the way a service markets/advertises itself may contribute to the appeal of a service to children. The London School of Economics has noted that children are "exceptionally vulnerable to commercial messaging"

[775] ONS, 2020. Children's online behaviour in England and Wales.
[776] UKCCIS, 2017. Children's online activities, risks and safety.
[777] GCHQ, DCMS, 2020, The Verification of Children Online: Phase 2 Report; Ofcom, 2024. Children and Parents: Media Use and Attitudes 2024.
[778] Ofcom, 2023. Children's Media Lives.
[779] ICO, 'Likely to be accessed' by children – FAQs, list of factors and case studies. [accessed 1 February 2024].

because "their ability to effectively understand persuasive messages in advertising has not yet fully developed".[780]

A3.30 The ICO's guidance on its Children's code states that providers should consider how they market, describe, and promote their service, specifically "whether advertisements on your service, including third party advertisements, are directed at or are likely to appeal to children. You may have information, including some provided to or by advertisers, such as number of clicks on ads that show an interest in child-focused advertising".[781] In their response to our 2023 call for evidence, ACT - The App Association noted that relevant factors may include ads targeted at places children may frequent and the language of the advertising/website/branding.[782]

A3.31 Carnegie UK noted in its response to our 2023 CFE that services or apps heavily marketed to children via host channels/accounts run by celebrities or influencers is a factor reflecting access by children.[783]

A3.32 The Molly Rose Foundation noted in its response to our 2023 CFE that providers should not be considered in isolation as one service is often used to cross-promote another service, which may also encourage children to set up accounts on additional services.[784]

A3.33 We have also included this in our Children's Access Assessments Guidance given that advertising-related data can be a factor in assessing whether the service is likely accessed by children. For example, if child-focused advertisers seek out the service, or if the service actively markets itself to child-focused advertisers.

A3.34 We have included a service's growth strategy as a consideration too, given that user growth may directly reflect an increase in children using the service or an increased likelihood of a service appealing to children. A comparative example may be taken from Generative AI. Ofcom research conducted in June 2024, found that 54% of online children in Britain aged 8-15 said they had used a Generative AI tool in the past year. ChatGPT, which launched in November 2022, was the most popular generative AI tool among this age group; it had been used by 37% of online 8-15-year-olds in the past year.[785] This reflects that a rapid user base expansion can encompass a growth in children's engagement as well.

A3.35 We have included this factor in the Children's Access Assessment Guidance because it demonstrates the intent and strategy of the service and by virtue of that, the types of users the service is aimed at. A provider will be aware of whether their service targets children,

---

[780] London School of Economics, 2022. Legal, honest and truthful: Advertising to children in the age of influencers. [Accessed 1 February 2024].
[781] ICO, 'Likely to be accessed' by children – FAQs, list of factors and case studies.
[782] ACT – The App Association response to 2023 Protection of Children Call for Evidence.
[783] Carnegie UK response to 2023 Protection of Children Call for Evidence.
[784] Molly Rose Foundation response to 2023 Protection of Children Call for Evidence.
[785] Ofcom, Online research panel poll: Generative artificial intelligence, June 2024. Question 1: When did you last use each of the following Generative AI tools? Base: GB internet users age: 8-15 (1051). The survey asked respondents about their use of 16 Generative AI tools: ChatGPT; ChatGPT Plugin; My AI on Snapchat, Google Gemini, Microsoft CoPilot, DALL-E, Midjourney, Character.AI, Scribe, AlphaCode, Quillbot, Synthesia, Claude from Anthropic, Perplexity, Stability's AI tools and Grok on X.

proactively or indirectly. Evidence available internally, marketing and growth strategies, will be useful sources of information for services carrying out this assessment.

A4. Glossary

Term	Meaning
2003 Act	Communications Act 2003 https://www.legislation.gov.uk/ukpga/2003/21/contents
Access control	Technical mechanism(s) which prevents users who have not been age assured, or having been age assured, did not meet the requirements of the age assurance process, from accessing a service (or part of it) or certain content.
Accuracy (ACC)	The fraction of the predictions the model got right. The formula is ACC = (TP + TN) / (TP+ TN + FP + FN).
Act	Online Safety Act 2023 https://www.legislation.gov.uk/ukpga/2023/50/contents
Age assurance	A collective term for age verification and age estimation.
Age assurance method	An age assurance method refers to the particular system or technology that underpins an age assurance process.
Age assurance process	An age assurance process refers the end-to-end process through which the age assurance method or combination of methods are implemented to determine whether or not a user is a child. The effectiveness of an age assurance method will depend on how it is implemented, including whether by itself or in combination with other methods.
Age assurance report	The Act requires Ofcom to produce a report about the use of age assurance, assessing how providers of regulated services have used age assurance for the purpose of compliance with their duties, how effective the use of age assurance has been for that purpose, and whether there are factors that have prevented or hindered the effective use of age assurance.[786]
Age estimation	A form of age assurance designed to estimate the age or age-range of the user[787], for example using facial age estimation.
Age check	An individual instance where a user is required to undergo an age assurance process.

[786] Section 157 of the Act.
[787] Section 230(3) of the Act.

Term	Meaning
Age verification	A form of age assurance designed to verify the exact age of the user[788], for example using a form of identity documentation.
App store report	The Act[789] requires Ofcom to produce a report about the use of app stores by children, by January 2027, including an assessment of the role app stores play in children encountering content that is harmful to children (including harmful search content and online pornography) and the potential child safety benefits of introducing age assurance.
Child	A person under the age of 18.[790]
Child user	A user under the age of 18.
Children's access assessment	A process that all Part 3 services in scope of the Act must carry out to determine whether they are likely to be accessed by children.
Children's Access Assessments Guidance	Guidance for Part 3 services on children's access assessments, published alongside this Statement.
Children's Risk Assessment Guidance	Guidance for Part 3 services on children's risk assessments, to be published alongside our Protection of Children Codes in April 2025.
Cumulative score (CS)	An aggregated score that is calculated by summing the individual score across over a period of time/category etc.
December 2023 Part 5 Consultation	"Guidance for service providers publishing pornographic content", published by Ofcom on 5 December 2023
December 2024 Statement	"Statement: Protecting people from illegal harms online", published by Ofcom on 16 December 2024
False negative (FN)	An outcome where a model incorrectly predicts a negative class i.e., a user is under 18 and the model predicts their age 18 or over.
False negative rate (FNR) / Miss rate	Measures the proportion of FN against all negative predictions (i.e., FN and TP). FPR highlights the performance of the model in yielding FP results and this should be minimised. The formula is FNR = FN / (FN + TP).

[788] Section 230(2) of the Act.
[789] Section 161 of the Act.
[790] Section 236(1) of the Act.

Term	Meaning
False positive rate (FPR)	Measures the proportion of FP against all positive predictions (i.e., FP and TN). FPR highlights the performance of the model in yielding FP results and this should be minimised. The formula is FPR = FP / (FP + TN).
Functionalities	In relation to a U2U service, includes any feature that enables interactions of any description between users of the service by means of the service.[791] In relation to a search service, includes (in particular): (a) a feature that enables users to search websites or databases; (b) a feature that makes suggestions relating to users' search requests (predictive search functionality).[792] In practice, when referring to functionalities in the Register of Risks, 'functionalities' refers to the front-end features of a service. For U2U services, 'functionalities' refers to features that enable interaction between users. 'Functionalities for search services' refers to features that enable users to search websites or databases, as well as predictive search functionalities that suggest search requests to users.
Generative artificial intelligence ("Generative AI")	Artificial intelligence models that can create text, images, audio and videos in response to a user prompt.
Highly effective age assurance (HEAA)	Methods of age assurance that are of such a kind and implemented in such a way that is highly effective at correctly determining whether or not a particular user is a child.
May 2024 Consultation	"Protecting children from harms online", published by Ofcom on 8 May 2024.
Mean absolute error (MAE)	The central value of the absolute error. It describes the average discrepancy between a user's technology determined age and their actual age, ignoring whether it is an over- or under-estimation. It is calculated by summing the absolute errors for a given number of absolute errors, then dividing this by the number of absolute errors. The formula is MAE = (1/n) Σ(i=1 to n) $\|y - x\|$ where n = number of observations in the dataset, y = is the true value, x = is the predicted value.

[791] Section 233(1) of the Act. Please refer to section 233(2) of the Act for a non-comprehensive list of U2U functionalities

[792] Section 233(3) of the Act.

Term	Meaning
Mean absolute percentage error (MAPE)	A metric that used to measure the accuracy in a regression analysis, this is useful where relative errors (age range estimations) are more meaningful than absolute errors. M = (1/n) Σ(t=1 to n)|(At – Ft) / At) |* 100 Where n = number of times the summation iteration happens, At = actual value and Ft = forecast value.
Non-designated content	Content not within Primary Priority Content or Priority Content of a kind which presents a material risk of significant harm to an appreciable number of children in the UK.
Outcome error parity	Outcome error parity is a measure designed to compare how an age assurance process outcome impacts users in different groups, both positively and negatively, and/or how often these different groups of users are subjected to errors.
Part 3 service or regulated search service	Refers to a search service that falls within the definition of section 4 of the Act.
Part 3 service or regulated user-to-user service	A user-to-user service, as defined in section 4 of the Act.
Part 5 service	An internet service falling within section 80(2) of the Act, which service displays or publishes certain pornographic content.
Part 3 HEAA Guidance	Guidance for Part 3 services on highly effective age assurance, published alongside this Statement.
Part 5 Guidance	Guidance for service providers publishing pornographic content, published alongside this Statement.
Pornography services	Services whose principal purpose is the hosting or dissemination of pornographic content and who host user-generated pornographic content.
Priority content (PC)	Content which is abusive or incites hatred, bullying content, and content which encourages, promotes, or provides instructions for violence, dangerous stunts and challenges, and self-administering harmful substances.
Primary priority content (PPC)	Pornographic content, and content promoting, encouraging or providing instructions for suicide, self-harm or eating disorders.
Protection of Children Codes	Services likely to be accessed by children are required by the Act to use proportionate safety measures to keep them safe. Our Protection of Children Codes will provide a set of safety measures that online services can take to help them meet their duties under the Act.

Term	Meaning
Provider	"The entity that has control over which content is published or displayed on the service." Where an individual or individuals have control over which content is published or displayed, rather than an entity, "the provider of the service is to be treated as being that individual or those individuals."[793] "The provider of an internet service that is generated by a machine is to be treated as being the entity that controls the machine (and that entity alone.)" "If no entity controls the machine, but an individual or individuals control it, the provider of the internet service is to be treated as being that individual or those individuals."[794]
Provider pornographic content	In relation to an internet service, "pornographic content that is published or displayed on a service by the provider of the service or by a person acting on behalf of the provider, including pornographic content published or displayed on the service by means of – a) software or an automated tool or algorithm applied by the provider or by a person acting on behalf of the provider, or b) an automated tool or algorithm made available on the service by the provider or by a person acting on behalf of the provider."[795]

[793]Section 226(8)-(9) of the Act.
[794] Section 226 (10)-(11) of the Act.
[795] Section 79(2) of the Act.

Term	Meaning
Published or displayed	Content in this context particularly includes references to pornographic content that is – a) "only visible or audible to users as a result of interacting with content that is blurred, distorted or obscured (for example, by clicking on such content), but only where the pornographic content is present on the service;" b) "embedded on the service," and; c) "generated on the service by means of an automated tool or algorithm in response to a prompt by a user and is only visible or audible to that user (no matter for how short a time.)"[796] It does not include pornographic content that – a) "appears in search results of a search service or a combined service,"[797] or b) "is user-generated content in relation to that service."[798]
Regulated provider pornographic content	Provider pornographic content other than content that – a) "Consists only of text, or b) Consists only of text accompanied by – • A GIF which is not itself pornographic content, • An emoji or other symbol, "or • A combination of (i) and (ii),[799] or • "Consists of a paid-for advertisement."[800]
Self-declaration	A process where the user is asked to provide their own age. This could be in the form of providing a date of birth to gain entry to a service or by ticking a box to confirm a user is over a minimum age threshold.

[796] Section 79(6)(a) of the Act.
[797] Section 79(6)(b) of the Act.
[798] Section 79(7) of the Act.
[799] Section 79(4) of the Act.
[800] Section 79(5) of the Act.

Term	Meaning
Service provider	The entity that has control over which content is published or displayed on the service. Where an individual or individuals have control over which content is published or displayed, rather than an entity, "the provider of the service is to be treated as being that individual or those individuals."[801] "The provider of an internet service that is generated by a machine is to be treated as being the entity that controls the machine (and that entity alone.)" "If no entity controls the machine, but an individual or individuals control it, the provider of the internet service is to be treated as being that individual or those individuals."[802]
Standard deviation (SD)	A measure of variation or dispersion of the dataset relative to the mean. A low SD suggests datapoints closer to the mean, whereas a high SD suggests datapoints are more dispersed. s = ∑((X − MAE)^2/(n − 1)) where X = is the i*th* point in the dataset, MAE = is the mean absolute error, and n = the number of datapoints in the dataset.
True positive	An outcome where a model correctly predicts a positive class i.e., a user is under 18 and model predicts their age as under 18.
True positive rate (TPR) / Recall	For the purpose of age assurance, this measures the proportion of TP predictions out of all actual positive instances (i.e., TP and FN). This metric highlights the model's performance in correctly identifying positive cases. The formula is TPR = TP / (TP + FN).
User-generated content	Content that is "generated directly on the service by a user of the service or uploaded to or shared on the service by a user of the service" and, "that may be encountered by another user, or other users, of the service by means of the service."[803]
User-to-user (U2U) services	An internet service on which users of the service can generate, upload and/or share content, which can then be encountered by other users of the service.
Virtual private network (VPN)	The creation of a private network over a public internet connection.
VSPs	Video-sharing platforms.

[801] Section 226(8)-(9) of the Act.
[802] Section 226(10)-(11) of the Act.
[803] Section 55(3) of the Act.