Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services

Annex 2

Published 5 December 2023

Contents

Section

Annex

1. Overview

What this guidance covers

This guidance is for service providers that display or publish pornographic content on their online services to help them comply with their regulatory duties under the Online Safety Act 2023 ('the Act'). These duties include a requirement for service providers to implement age assurance to ensure that children are not normally able to encounter pornographic content displayed or published on their service. [1, 2]

This document gives guidance on:

- assessing whether a service is in scope of the Part 5 duties;
- examples of kinds of age verification and age estimation that may be suitable for the purposes of compliance, and criteria that service providers should fulfil to ensure the age assurance implemented is highly effective at correctly determining whether or not a particular user is a child;
- 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 of privacy law in their written record; and
- 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.

A summary of the duties and recommendations covered in this guidance is set out on the next page.

Summary of service providers' Part 5 duties

✓ Implement age assurance, for example using one or more of the methods listed in Section 4 of the guidance.

✓ Ensure that the age assurance process used is: (a) of a kind that could be highly effective at correctly determining whether or not a user is a child; and (b) used in such a way that it is highly effective at correctly determining whether or not a user is a child (for example by considering the criteria set out in Section 4 of the guidance).

✓ Ensure that, by using the age assurance process in question, children are not normally able to encounter regulated provider pornographic content on the service (i.e., by using an effective access control measure).

✓ Keep an easily understandable written record of:

- the kinds of age assurance used and how they are used by the service provider or a third-party age assurance provider;

[1] We use the term '**age assurance'** to refer to both age verification and age estimation. We provide further detail on definitions in Annex 1 of this document.
[2] Section 81(2) of the Online Safety Act 2023.

- how the service provider has had regard to privacy and data protection laws when deciding which age assurance process to use and how.

✓ Produce a publicly available summary of the parts of the written record relating to implementing highly effective age assurance, including the age assurance method(s) the service provider is using and how.

What service providers should do to support compliance with their 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.

+ Implement any techniques to mitigate against attempts at 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, 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 Information Commissioner's Office (ICO).

+ Refrain from hosting, sharing or permitting content that directs or encourages child users to circumvent the age assurance process or access controls.

2. Introduction

2.1 The Act creates a new regulatory framework with the general objective of making regulated internet services safer for users in the United Kingdom (UK), particularly for children. To achieve this, it includes specific duties on service providers that display or publish pornographic content to implement age assurance on their online services to ensure that children are not normally able to encounter such content (**'the Part 5 duties'**). We use **'age assurance'** in this context to refer to both age verification and age estimation.

2.2 Age assurance for the purposes of compliance with the Part 5 duties must be of a kind and used in a way that is **highly effective at correctly determining whether or not a user is a child**.

2.3 We refer to service providers that display or publish pornographic content on their online services as **'service providers'** and the services within scope of Part 5 of the Act as **'regulated services'** throughout this guidance.

How to use this guidance

2.4 This guidance is to assist service providers in complying with the Part 5 duties.[3] 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.

2.5 Below, we set out an overview of the aspects of guidance that we cover in each section of this document.

Section 3: The scope of the Part 5 duties

2.6 Section 3 provides guidance to service providers as to how they can assess whether their services fall in scope of Part 5. This includes guidance on:

i) assessing whether content is pornographic content which is regulated under Part 5 of the Act (referred to as **'regulated provider pornographic content'**);
ii) exemptions to Part 5 under the Act; and
iii) assessing whether a service has links to the UK.

Section 4: The age assurance duties

2.7 Section 4 provides guidance to service providers on how to use age assurance to ensure that children are not normally able to encounter regulated provider pornographic content on their regulated services. This includes:

i) a non-exhaustive list of age assurance methods that we consider could be highly effective at correctly determining whether or not a user is a child, and those that we consider at present are not capable of being highly effective;

[3] Ofcom has a duty under Section 82(2) of the Act to provide guidance for service providers to assist them in complying with their duties set out in Part 5 of the Act. The Act requires Ofcom's guidance to include several elements, including 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, and examples of circumstances in which Ofcom is likely to consider that a provider has not complied with its duties.

ii) criteria the age assurance process should fulfil to ensure that it is highly effective at correctly determining whether or not a child is user, and guidance on how to fulfil these criteria;
iii) principles that service providers should consider to ensure that the age assurance process is easy to use and that, as far as possible, adult users are not unduly prevented from accessing legal content; and,
iv) examples of circumstances where we are likely to consider a provider has not complied with these duties.

Section 5: The record-keeping duties

2.8 Section 5 provides guidance to service providers on the duties relating to record-keeping. This includes guidance on:

i) how to keep a written record;
ii) the content which must be included in the service provider's written records and what must be summarised in a publicly available statement;
iii) how service providers can have regard to protecting users' privacy; and,
iv) circumstances where we are likely to consider a provider has not complied with its duties.

Section 6: Our approach to assessing compliance with the age-assurance and record-keeping duties

2.9 Section 6 provides an explanation of the approach we will take to assessing compliance with the Part 5 duties. This includes:

i) our general approach to enforcement of the Act; and,
ii) the principles that we will apply when determining whether a service provider has complied with each of its Part 5 duties.

3. The scope of the Part 5 duties

3.1 An internet service falls within the scope of Part 5 of the Act if:

i) regulated provider pornographic content is published or displayed on the service ('condition 1');
ii) the service is not out of scope of Part 5 or exempt ('condition 2'); and,
iii) the service has links to the UK ('condition 3').

3.2 Condition 1 relates to the **type of content** which is published or displayed on the service. Condition 2 relates to the **types of service** which are out of scope of Part 5 or exempt, including on-demand programme services. Condition 3 relates to the intended or actual **user base of the service**.

3.3 This section provides an overview of each of these conditions which determine whether a regulated service is in scope, with reference to the relevant statutory definitions. We also provide some high-level examples to assist service providers in understanding how these definitions apply.

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

What pornographic content falls within Part 5?

3.4 Part 5 of the Act applies to pornographic content which is published or displayed on an online service by the provider of the service, or by a person acting on behalf of the provider. For the purposes of Part 5, the pornographic content which is subject to regulation is called '**regulated provider pornographic content.**'

3.5 Pornographic content is defined in the Act 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."[4]

> Pornographic content might include any content which would fall under the British Board of Film Classification's (BBFC) R18 category, which is "primarily for explicit works of consenting sex or strong fetish material involving adults." [5] However, other content of a strong sexual nature that seeks to sexually arouse or stimulate, that would not fall in scope of this classification, may also be treated as pornographic.

3.6 Where pornographic content appears online, it will fall within the scope of Part 5 as regulated provider pornographic content if:

i) the content meets the definition for provider pornographic content as set out in section 79(2) of the Act; and,
ii) the content is not a category of pornographic content explicitly carved out from that definition; or,

[4] Section 236(1) of the Act.
[5] 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 23 November 2023].

iii) the content is not otherwise exempted or excluded.

3.7 The definition for regulated provider pornographic content includes pornographic content published or displayed on the service by means of:

i) a software or an automated tool or algorithm applied by the provider or a person acting on behalf of the provider, or
ii) an automated tool or algorithm made available on the service by the provider or a person on behalf of the provider.[6]

The definition of regulated provider pornographic content encompasses content in a range of forms, including still and moving images, audio and audio-visual content. This might include, for instance, a livestream or explicit photos of sexual activity.

What pornographic content falls outside of Part 5?

3.8 Not all pornographic content is included under the definition of regulated provider pornographic content. The following content is expressly excluded:

i) Pornographic content that is user-generated content in relation to an internet service;[7]
ii) Pornographic content that-

- consists only of text, or
- 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);[8]

iii) Content if it consists of a paid-for advertisement.[9]

3.9 Part 3 of the Act sets out obligations for user-to-user services, including the requirement for regulated user-to-user services that allow pornographic content on their service to use highly effective age assurance to prevent children from encountering it.[10]

3.10 Provider pornographic content may be present on different types of online service, including those which are predominantly user-to-user services. Such services will be subject to the Part 5 duties in relation to the pornography that the provider itself (or a person acting on behalf of the provider) publishes or displays on the service.

---

[6] See section 79(3) and (6)(a) of the Act.
[7] Section 79(7) of the Act. For a definition of 'user-generated content' see section 55(3) and (4) of the Act.
[8] Section 79(4) of the Act.
[9] Section 79(5) of the Act. An advertisement is a 'paid-for advertisement' in relation to an internet service if -
a) the provider of the service receives any consideration (monetary or non-monetary) for the advertisement (whether directly from the advertiser or indirectly from another person), and
b) the placement of the advertisement is determined by system or processes that are agreed between the parties entering into the contract relating to the advertisement. See section 236(1) of the Act.
[10] See section 12 of the Act. All regulated user-to-user services that are likely to be accessed by children must use highly effective age assurance to prevent children from encountering primary priority content that is harmful to children, including pornographic content (under section 61(2)), except where such content is prohibited on the service for all users.

What does "published or displayed by the provider on its internet service" mean?

3.11 For the purposes of Part 5, the circumstances in which pornographic content will be treated as published or displayed on a service include where the pornographic content:

i) 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;
ii) is embedded on the service; and,
iii) 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).[11]

3.12 Pornographic content which appears in the search results of a search engine or a combined service is not treated as published or displayed on the search service or combined service in question for the purposes of Part 5 of the Act. [12] These services will be subject to obligations in Part 3 of the Act, including the children's risk assessment and safety duties in, as applicable, sections 11 to 13 and 28 to 30 of the Act.

3.13 The duties in Part 5 apply where pornographic content is published or displayed by a provider of an internet service (or on behalf of such a provider) on that internet service. Where an entity or individual has control over which content is published or displayed on an internet service, that entity or individual will be treated as the provider of the internet service, unless the service in question is a user-to-user service or a search service.[13, 14]

We are likely to consider a service provider to have exercised control over the pornographic content appearing on its service where it exercises editorial control over the nature, selection or presentation of the content. For example, where 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.

Similarly, where 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.

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. For example, while tube sites are often predominantly user-to-user services (i.e., predominantly comprised of user-generated pornographic content), a provider of a tube site may itself

[11] Section 79(6)(a) of the Act.
[12] In relation to a search service, a 'search result' means "content presented to a user of the service by operation of the search engine in response to a search request made by the user" under section 57(3) of the Act. A 'combined service' is a "regulated user-to-user service that includes a public search engine" under section 4(7) of the Act.
[13] Section 226(8) and (9) of the Act.
[14] In the case of a user-to-user service, the provider is the entity or individual with control over who can use the site (section 226(2) and (3) of the Act); in the case of a search service, the provider is the entity or individual which has control over the operations of the search engine (see section 226(3) and (4) of the Act).

make some pornographic content available on that site.[15] 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, for instance if that part of the service is an on-demand programme service, as explained in paragraph 3.16 below.

3.14 As set out in paragraph 3.11 above, pornographic content will also be treated as published or displayed on a service when it is generated on the service by means of an automated tool available in the service, such as a generative artificial intelligence tool (GenAI) or an algorithm in response to a prompt by a user. In this case, the provider of the relevant internet service is the entity or person with control of, and making available, the tool or algorithm in question.[16]

Condition 2: The service is not exempt

Which services are outside the scope of Part 5 or exempt?

3.15 There are certain types of services which fall outside the scope of Part 5. As noted above, user-generated content on a user-to-user service (or combined service) and the search results on a search service (or combined service), are outside the scope of Part 5 and instead are regulated under the provisions of Part 3 of the Act.

3.16 Some providers of pornographic content may provide such content through an 'on-demand programme service.' This might include, for instance, a pornographic subscription service where editorial decisions about that service are made in the UK and the provider of the service has its head office in the UK. Part 5 does not apply in relation to a service to the extent it is an on-demand programme service within the meaning of section 368A of the Communications Act 2003 ('CA03').[17] Ofcom has provided guidance which sets out the statutory criteria for determining whether or not a service is an on-demand programme service. On-demand programme services are regulated under Part 4A of the CA03, and Ofcom has set out Rules and Guidance for providers of on-demand programme services.

3.17 We have also set out guidance for on-demand programme service providers on measures to protect users from harmful material, which includes guidance on the specific rules relating to the protection of under-18s from harmful material.

3.18 There are also exemptions for services within the scope of Schedule 1 or Schedule 9 of the Act, the principal effect of which is to remove internal business services (e.g., intranet services) from Part 5 provided they meet the specified requirements in the Schedules.

[15] The BBFC defines tube services as free-to-access vide-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.
[16] Section 226(10) and (11) of the Act.
[17] Section 80(6) of the Act.

Condition 3: The service has links to the UK

3.19 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:

a) The service has a significant number of UK users, or
b) The UK forms one of the target markets for the service, or the only target market.[18]

What is a "significant number of UK users"?

3.20 The Act does not define what is meant by a 'significant number' of UK users for the purposes of considering the 'UK links' condition. Service providers should be able to explain their judgement, especially if they think they do not have a significant number of UK users.

3.21 Under the Act, where a user of a service is an individual, they must only be counted as a user where they are in the UK. Where the user is an entity, it must only be counted where that entity has been formed or incorporated in the UK.[19] A user also does not need to be registered to use the service in question to be counted as a user for the purposes of determining whether there is a significant number of UK users.[20]

3.22 Certain users should not be counted for these purposes where they are acting in the course of the provider's business.[21] Whatever methodology a service uses to calculate user numbers, we expect providers to be able to distinguish between these types of users for the purposes of determining whether there is a significant number of UK users on the service.

When will the UK be a target market for a service?

3.23 A target market is a specific group of people (or organisations) that a provider is aiming its service toward. There are a variety of factors which could mean the UK is a target market for a service, for instance in the way it designs, promotes, or receives revenue from, the service. For the avoidance of doubt, even if the UK is not a target market, a service could still meet the 'UK links' condition if it has a significant number of UK users.

[18] Section 80(4) of the Act.
[19] Section 227(1) of the Act.
[20] Section 227(2) of the Act.
[21] See section 227(3) and (4) of the Act.

4.The age assurance duties

Introduction to the age assurance duties

4.1 The Act imposes the following core duties relating to age assurance on service providers in scope of Part 5:

> 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;[22] and
>
> The age verification or age estimation 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. [23]

4.2 Throughout this guidance, we refer to the duties in paragraph 4.1 as the **'age assurance duties.**' The effect of these duties is to require service providers within scope of Part 5 to deploy age assurance which is highly effective at determining whether or not a user is a child. Whenever a child is identified, the provider must ensure that they are not able to encounter regulated provider pornographic content on the service. This means that the service provider must implement effective access controls to prevent users who have been identified by the age assurance process as children from encountering such content on the service (for example, by denying them access to any further sections of the service).

4.3 In this section, we provide some examples of circumstances in which we are likely to consider that a service provider has not complied with the age assurance duties ('examples of non-compliance'). In considering whether there may be a failure to comply with the duty to ensure that children are not normally able to encounter regulated provider pornographic content, we will be mindful of the fact that it may be possible for users to circumvent the age assurance process or access control mechanisms that the provider has put in place to meet its duties.

4.4 We expect service providers to take steps to mitigate against, and refrain from promoting, any circumvention techniques which are easily accessible to children and where it is reasonable to assume they may use them. In addition, service providers should not host or permit content on their service that directs or encourages child 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 relevant processes.

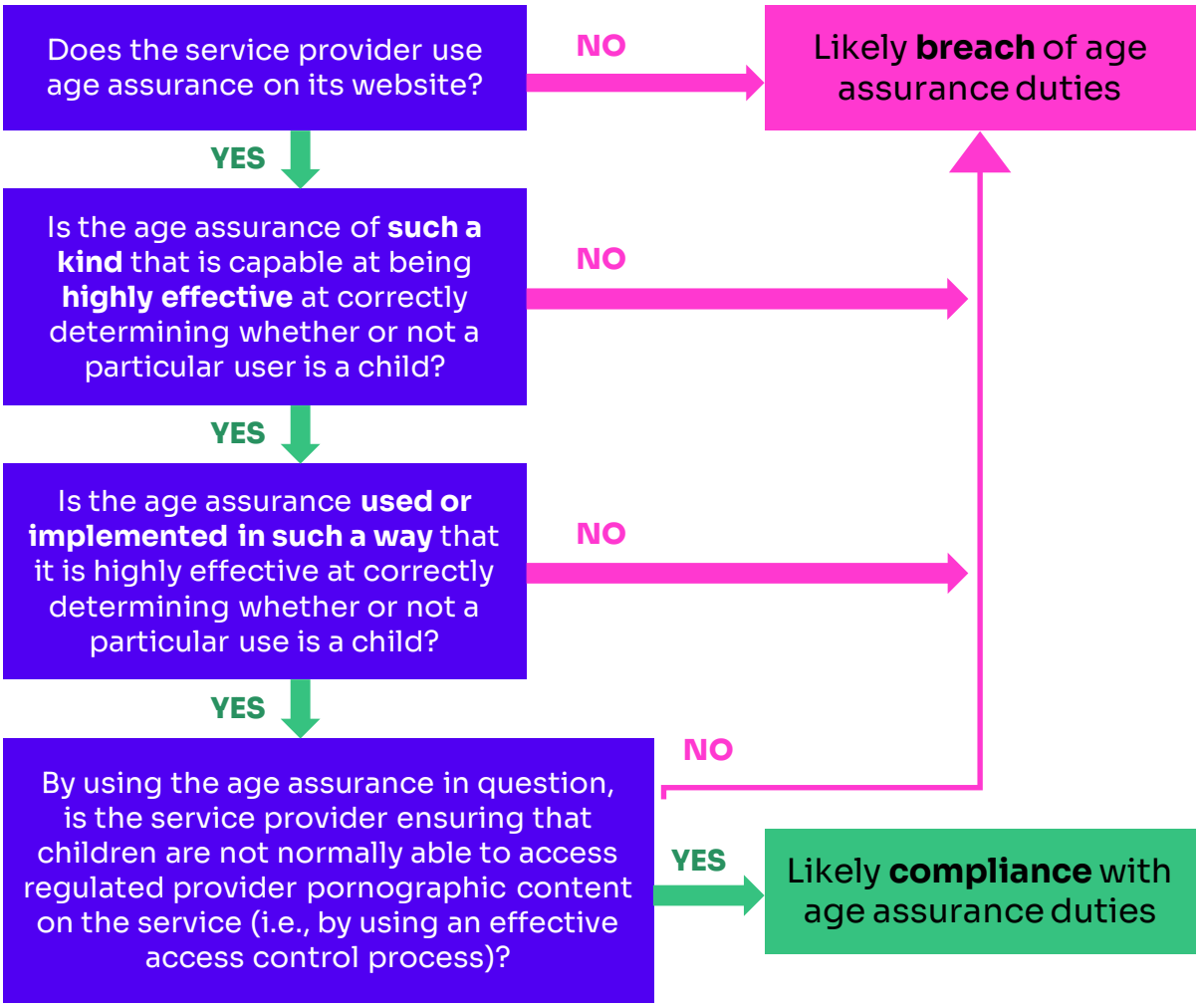
[22] Section 81(2) of the Act.
[23] Section 81(3) of the Act.

Example of non-compliance

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.

4.5 The following flow diagram shows – at a high level – the analytical framework Ofcom will use when assessing whether both of the age assurance duties have been met.

Figure 4.1: Analytical framework for assessing in-scope services' compliance with the age assurance duties.



4.6 In this section, we:

i) outline the kinds of age assurance that we consider could be highly effective at correctly determining whether or not a user is a child, and those that are not capable of doing so;

ii) explain how service providers can use age assurance in such a way that is highly effective at correctly determining whether a user is a child by fulfilling certain criteria; and

iii) set out certain principles that service providers should consider to ensure that the age assurance process is easy to use, and does not unduly prevent adult users from accessing legal content, where possible.

Age assurance methods and processes

4.7 Throughout this guidance, we refer to age assurance **methods** and **processes.**

4.8 An **age assurance method** refers to the particular system or technology that underpins an age assurance process.

4.9 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. While some methods are better than others at establishing whether 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. The age assurance process as a whole needs to be highly effective at correctly determining whether a particular user is a child.

Placement of age assurance

4.10 To ensure that children are not normally able to encounter pornographic content, service providers must ensure that no pornographic content on their regulated service can be accessed by users before they verify their age. This means implementing age assurance at the point of entry to the site or ensuring that no regulated provider pornographic content is visible to users on entering the site before they have completed the age check.

Example of non-compliance

Regulated provider pornographic content is visible to users on the regulated service prior to or during the process of completing an age check.

Kinds of age assurance

4.11 Below, we set out a non-exhaustive list of kinds of age assurance that we consider could be highly effective at correctly determining whether or not a user is a child. We recognise that age assurance methods are developing at pace and this list may expand in time.

4.12 The kinds of age assurance in this list may be referred to by different names, and each kind may be implemented in a number of ways. We have used high-level descriptions to assist service providers in understanding the options that are available to them, but it is for each provider to consider which age assurance methods and processes will be most appropriate for complying with the duties.

4.13 We also provide examples of methods that we do not consider are capable of being highly effective at correctly determining whether or not a user is a child. Where a service provider

relies on these measures alone to determine whether or not a user is a child, we would be likely to consider that the provider has not complied with either of the age assurance duties.

4.14 All age assurance methods involve the processing of personal data. As such, they are subject to the requirements of the UK's data protection regime. The ICO has issued guidance on how these requirements should be met, as outlined in paragraphs 5.20 to 5.23, which will assist service providers to implement age assurance while protecting user privacy in line with the data protection regime.

Kinds of age assurance that could be highly effective

4.15 **Open banking.** This works by accessing the information a bank has on record regarding a user's age, with the user's consent. Confirmation of whether or not the user is over 18 is shared with the relying party.[24] The user's date of birth is not shared with the relying party, nor is any other information.

4.16 **Photo-identification (photo-ID) matching.** This works by capturing relevant information from an uploaded photo-ID document and comparing it to an image of the user at the point of ID upload to verify that they are the same person.

4.17 **Facial age estimation.** This works by analysing the features of a user's face to estimate their age.

4.18 **Mobile-network operator (MNO) age checks.** Each of the UK's MNOs have agreed to a code of practice whereby a content restriction filter (CRF), which prevents children from accessing age-restricted websites over mobile internet, is automatically applied on pay-as-you-go and contract SIMs. Users can remove the CRF by proving they are an adult.[25] MNO age checks rely on checking whether the CRF on a user's mobile phone has been removed. If the CRF has been removed, this indicates that the recorded user of the device is over 18. Confirmation of whether or not the recorded user is over 18, based on the status of the CRF, is shared with the relying party.

4.19 **Credit card checks.** In the UK, you must be 18 or over to obtain a credit card, therefore, credit card issuers are obliged to verify the age of applicants before providing them with a credit card. Credit-card based age checks work by asking a user to input their credit card details, after which a payment processor sends a request to check the card is valid by the issuing bank. Approval by the issuing bank can be taken as evidence that the user is over 18.[26]

4.20 **Digital identity wallets.** Digital identity wallets enable users to verify and securely store their attributes, such as age, in a digital format. This verification may take place using a variety of methods, including those listed above. Once their identity or an attribute of their identity has been verified and stored in the wallet, a user may choose to share individual attributes, such as their age, or their status as an adult, with a relying party.

[24] Relying party refers to the service that is trying to establish the age of the user. In this context, the relying party is likely to be the regulated service.
[25] There are several ways to remove a CRF, depending on the MNO.
[26] Possession of credit card details is not guaranteed to be evidence that the user with the details is the person who took out the credit card.

Kinds of age assurance that are not capable of being highly effective

4.21 **Self-declaration of age:** The Act states that measures which require users to self-declare their age are not to be regarded as age assurance. [27] There is evidence to support this, and such methods are therefore not appropriate for the purposes of compliance with Part 5 duties. These include:

i) asking a user to input their date of birth without any further evidence to confirm this information; or
ii) asking a user to tick a box to confirm that they are 18 years of age or over.

4.22 **Age verification through online payment methods which do not require a user to be over the age of 18.** For example, Debit, Solo or Electron cards, or any other card where the card holder is not required to be 18.

4.23 **General contractual restrictions on the use of the regulated service by children**. For example:

i) including as part of the terms of service a condition that prohibits users who are under 18 years old from using the regulated service, without any additional age assurance;
ii) general disclaimers asserting that all users should be 18 years of age or over; or
iii) warnings on specific content that the content is suitable for over 18s.

Example of non-compliance

The service provider relies solely on self-declaration, general contractual restrictions or payment methods which do not require a user to be over 18, or a combination of these, to determine the age of users.

Criteria to ensure an age assurance process is highly effective

4.24 As explained above, to ensure children are not normally able to encounter regulated provider pornographic content, service providers need to: (a) choose an appropriate kind (or kinds) of age assurance; and (b) implement it in such a way that it is highly effective at correctly determining whether a user is a child.

4.25 We have set out some examples of kinds of age assurance that we consider could be highly effective at correctly determining whether or not a user is a child. However, to ensure that an age assurance process is, in practice, highly effective at correctly determining whether or not a user is a child, service providers should ensure that the process fulfils **each** of the following criteria:

a) it is technically accurate;
b) it is robust;
c) it is reliable; and
d) it is fair.

[27] Section 230(4) of the Act.

4.26 These criteria apply to the technical operation of the age assurance method. The below table provides a brief summary of the criteria, all of which are to be used by service providers to decide their approach to age assurance. We go into more detail about each of the criteria below.

Figure 4.2: Summary table of the criteria service providers should fulfil and how they can do so.

Criteria	Practical steps to fulfil criteria
Technical accuracy: the degree to which an age assurance method can correctly determine the age of a user under test lab conditions.	Ensure the age assurance method(s) has been evaluated against appropriate metrics. Include details of the performance of the method(s) against the metrics in the written record (see Section 5 below). Consider implementing a 'challenge age' approach for age estimation methods (see box under paragraph 4.38 below).
Robustness: the degree to which an age assurance method can correctly determine the age of a user in unexpected or real-world conditions.	Implement age assurance processes that have undergone tests in multiple environments during development. Include details of this test process in the written record (see Section 5 below). 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.
Reliability: the degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.	Ensure that age assurance methods with a degree of variance have been suitably tested, and that ongoing performance is measured and monitored. Ensure that the evidence that the age assurance method uses is a from a trustworthy source. Where using methods that rely on identity documents, record details of which identity documents they require or accept in the written record.
Fairness: the extent to which an age assurance method avoids bias or discriminatory outcomes.	Ensure that, where relevant, age assurance methods have been trained on diverse datasets.

4.27 We recognise that different kinds of age assurance – or even the same kinds of age assurance provided by different companies – may perform more strongly in some of these criteria than others. For example, one age assurance method could produce a highly reliable result due to limited variance, but it may provide greater opportunities for children to circumvent, therefore reducing its robustness.

4.28 We 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. We recognise that in doing so, there may be trade-offs in how well individual age assurance methods perform against each of the criteria. 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 correctly determining whether or not a particular user is a child, to ensure that children are not normally able to encounter pornographic content on the regulated service.

4.29 Below, we explain the criteria, why they are important, and steps providers can take to have regard to them.

Technical accuracy

What is technical accuracy?

4.30 Technical accuracy describes the degree to which an age assurance method can correctly determine the age of a user under test lab conditions. In some cases, service providers may be in a position to conduct their own tests that are appropriate but generally our expectation is that they will need to make enquiries of third-party providers to ascertain the basis for assurances that their age assurance methods are technically accurate. We will expect providers to understand what tests have been conducted and the metrics which have been used to measure the results. Alternatively, this information may be available via testing carried out by an independent third party.

Why is technical accuracy important?

4.31 Technical accuracy is an indicator of the performance of an age assurance method. An age assurance method which performs poorly in test conditions will perform worse in a real-world deployment and is therefore very unlikely to be highly effective at correctly determining the age of users when deployed. This indicates that an alternative or additional age assurance method is likely to be required. Understanding the technical accuracy of the individual age assurance method(s) is therefore an important step in ensuring that the process as a whole is highly effective at correctly determining whether or not a particular user is a child.

How can service providers have regard to technical accuracy when implementing age assurance?

Ensure the method(s) has been evaluated against appropriate metrics

4.32 We expect service providers to evidence that they have taken steps to understand how technically accurate the age assurance method(s) they use is.

4.33 To understand the technical accuracy of an age assurance method, service providers should ensure it has been evaluated against appropriate metrics. Age assurance methods either produce:

a) A binary result (for example, categorising users as either over or under the age of 18).
b) A continuous result (for example, providing an estimation of the user's age).[28]

[28] The estimation of the user's age will usually be accompanied by a confidence interval or range, which conveys the algorithm's level of uncertainty regarding the prediction. For example, where an age estimation method predicts that a user is 25 years old with a confidence interval of ±2 years, this means that the method estimates the user's age to fall within the range of 23 to 27 years.

4.34 Service providers should ensure that the appropriate metrics have been assessed to allow them to determine whether the method they have developed or are utilising from a third-party vendor is technically accurate enough to be considered highly effective. For age assurance methods producing binary results this could include a range of metrics e.g., the True Positive Rate (TPR), False Positive Rate (FPR), and False Negative Rate (FNR).

4.35 For age assurance methods that produce continuous results this could include a range of metrics e.g., the Standard Deviation, Mean Absolute Percentage Error (MAPE), and Cumulative Score (CS).[29]

4.36 As explained above, these metrics could be derived from the providers' own internal testing (if feasible), from the testing that third party providers have done, or from testing by an independent third party.

4.37 To demonstrate consideration of technical accuracy, service providers should record details of the assessment they made in relation to the above requirements. For further information on keeping a written record, providers should refer to Section 5.

4.38 We expect that the technical accuracy and testing practices of age assurance methods will continue to improve in years to come. Keeping a written record of the technical accuracy will help service providers to understand how the effectiveness of their process compares against new technologies that may come onto the market. 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.

Service providers could consider implementing a 'challenge age' approach for estimation methods which are not sufficiently technically accurate within a specific age range.

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 produces an output that could have been subject to error.[30]

A 'challenge age' approach is widely used offline when selling age-restricted products in retail environments, for example through the retailing strategy 'Challenge 25.'

Where a 'challenge age' approach is adopted in an online age assurance process, age estimation may be used in the first instance. The challenge age should be set according to the limits of the technical accuracy of that method. For example, where the age method has a variance of 7 years for users that are 18 years of age (i.e., it often estimates the user's age incorrectly by up to 7 years above or below 18), the challenge age should be set to 25. For users estimated to be over the age of 25, no additional verification will be required. Where the method estimates that the user's age is under the challenge age, the user could be required to undergo another age check by a second method that is more technically accurate for that age group.

[29] We define each of the metrics set out in the technical glossary in Annex 1 of this document.

[30] 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.

Implementing a process with a challenge age approach can help service providers to ensure that their age process overall is proportionate and highly effective at correctly determining whether or not a user is a child.[31]

Example of non-compliance

The age assurance process routinely fails to correctly determine whether or not a particular user is a child.

Robustness

What is robustness?

4.39 Robustness describes the degree to which an age assurance method can correctly determine the age of a user in unexpected or real-world conditions.

4.40 Common threats to robustness in the context of age assurance methods include:

i) **Conditions that change the quality or characteristics of the input** e.g., poor lighting, blurring, brightness, contrast, or positioning of the user in the image (relevant for methods reliant on visual input e.g., facial age estimation, photo-ID matching, etc); and,

ii) **Circumvention techniques that are easily accessible to children where it is reasonable to assume they may use them** (i.e., a child user uploading an image of an ID that does not belong to them).

4.41 Risks such as these can be mitigated by service providers taking steps to improve the robustness of their age assurance process.

Why is robustness important?

4.42 Conditions in the real-world will vary considerably to those in a test scenario.

4.43 If the age assurance method is not robust, there are likely to be discrepancies in how it performs across varying conditions. For example, the technical accuracy of the method might be lower where a low-quality camera is used. Therefore, such a method would not be highly effective at correctly determining whether or not a user is a child as it is not technically accurate in a varied set of conditions.

4.44 In addition, there may be circumvention techniques which are easily accessible to children and where it is reasonable to assume that children may use them. If the age assurance process is not robust, it will be more vulnerable to circumvention. Therefore, the service provider will not be able to ensure that children are not normally able to encounter pornographic content.

How can service providers have regard to robustness when implementing age assurance?

Where relevant, ensure the technology has been tested in a range of conditions

4.45 We expect service providers to implement age assurance processes that have undergone testing to ensure the process is highly effective in a range of conditions.

[31] ACCS, 2023, Measurement of Age Assurance Technologies. Part 2 – Current and short-term capability of a range of Age Assurance measures, p. 4.

4.46 Should service providers choose an age assurance method dependent on visual or audio input, they should ensure that the technology underpinning that method has been tested in multiple environments during its development, to minimise any discrepancies in the performance of the method in unexpected or real-world conditions.

4.47 Service providers could include details of this test process in their written record, as part of evidencing how they have chosen certain kinds of age assurance.

Mitigate circumvention attempts that are accessible to children where it is reasonable to assume that children may use them

4.48 While no age assurance method is likely to be effective all the time and in all circumstances, we expect service providers to make efforts to mitigate against methods of circumvention that are easily accessible to children, and where it is reasonable to assume that children may use them. The steps below relate to circumvention techniques which are specific to certain age assurance methods. We cover general attempts to circumvent the age assurance process or access control process above at paragraph 4.4.

4.49 Requiring a photo of the user at the point of ID upload when photo-ID matching can help to verify that the photo ID belongs to that user. Liveness 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.

4.50 Similarly, it is possible to obtain fake forms of identification of varying degrees of sophistication. A robust photo-ID check should not be capable of being easily circumvented, and as such, a photo-ID method should be able to detect basic levels of falsified documentation or manipulation that a child could create or obtain. Government-issued guidance on how to prove and verify someone's identity ('GPG45') provides some useful indicators on how a document can be scored to detect certain levels of faked documentation. To prevent the most basic levels of faked documentation getting through, this could align to a photo-ID method meeting at least level 2 checks from GPG45.[32]

Example of non-compliance

The service provider has not taken steps to mitigate against circumvention attempts which are easily accessible by children, and where it is reasonable to assume they may use them. For example:

- the service provider has implemented facial age estimation which allows children to upload a still image they have obtained of an adult; or

-the service provider has implemented photo-ID matching which easily allows children to verify their age using fake or manipulated ID documents.

Reliability

What is reliability?

4.51 Reliability describes the degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.

[32] Cabinet Office and Government Digital Service, 2023, Guidance – How to prove and verify someone's identity [accessed 23 November 2023]. Subsequent references to this document are referred to as 'GPG45.'

4.52 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.[33]

4.53 Strength of evidence describes the relative weight that should be afforded to the underlying data or documents used as evidence for a user's age.[34] 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.

Why is reliability important?

4.54 Without reproducibility, an age assurance method might prevent a child from encountering pornographic content in some circumstances, but not in others. Demonstrating that a method can account for variance and create reproducible outputs is an important element of ensuring that children are not normally able to encounter pornographic content online.

4.55 In addition, where age assurance does not rely on trustworthy age evidence, there is a risk that children are granted access to the regulated service based on evidence that wrongly suggests they are an adult.

How can service providers have regard to reliability when implementing age assurance?

Ensure that methods with a degree of variance have been suitably tested and that ongoing performance is measured and monitored

4.56 Age assurance methods that rely on statistical modelling or artificial intelligence, such as facial age estimation and photo-ID matching, are likely to produce outputs with a degree of variance. There are several reasons for this, including data variability and model complexity.

4.57 In addition, the performance of these specific methods may degrade over time due to 'model drift'. This is where the data the method has been trained on becomes less representative of the population using the age assurance method. For example, population demographics may shift over time resulting in a greater degree of variance.

4.58 In both these instances, we expect service providers to implement age assurance processes that have undergone regular testing to ensure that outputs are consistently produced when the method is presented with the same inputs.

4.59 This testing should be accompanied by regular monitoring and measurement of key performance indicators of the system.[35] Where necessary, root cause analysis and retraining should also be carried out where unexpected or unreliable predictions are being observed, particularly where such predictions may risk children being able to access adult content.

4.60 For other kinds of age assurance methods, including credit card age checks, open banking, and MNO age checks, outputs do not generally exhibit any variance of the type described above. In these cases, identical outputs should be produced when the method is presented

---

[33] Gundersen OE, Kjensmo S, 2018, State of the art: Reproducibility in artificial intelligence in Proceedings of the AAAI Conference on Artificial Intelligence 32(1), p. 1645.

[34] 'Strength' refers to evidence being harder to forge or counterfeit, as defined in GPG45.

[35] For example:

1) Age Verification Accuracy Rate (AVAR): the percentage of users correctly identified as belonging to the appropriate age group;
2) Age Verification Efficiency (AVE): the time taken to complete the age verification process;
3) Drift Threshold: establish predefined thresholds for AVAR and AVE beyond which significant model drifting is considered to have occurred.

with the same inputs. While reliability is less relevant for these methods, the service provider should still ensure that they fulfil the criteria of technical accuracy, robustness, and fairness.

Ensure that the evidence used is derived from a trustworthy source

4.61 We expect service providers to have confidence in the evidence that the age assurance method is relying on by considering, for example:

i) the nature and properties of any identity documents, profiles, accounts, data, etc. used as part of the age assurance process;
ii) the source of the underlying data or documents.

4.62 In assessing the nature and properties of the relevant evidence, service providers should identify features that they would expect to see in a reliable source. When deploying photo-ID matching, for example, these features might include that:

- the evidence has originated from a country or organisation that is recognised as trustworthy;
- the positioning of the photographs on the evidence does not suggest they have been edited or replaced;
- the layout or any logos look as expected; and/or,
- the visible security features are genuine.[36]

4.63 Where service providers use methods that rely on identity documents, they should record details of which identity documents are required in their written record, as part of evidencing how they have used certain kinds of age assurance.

Fairness

What is fairness?

4.64 Fairness describes the extent to which an age assurance method avoids or minimises unintended bias and discriminatory outcomes. It refers to the internal operation of an age assurance method, rather than external factors which are covered by the principles below.[37]

Why is fairness important?

4.65 If correctly implemented the age assurance duties should avoid: (a) child users being incorrectly identified as adult users; and (b) adult users being incorrectly identified as child users. As part of this, service providers should ensure an age assurance method does not produce discriminatory outcomes for certain groups, for instance, a lower degree of technical accuracy for users of a certain ethnicity when relying on facial estimation.

4.66 Implementing a fair age assurance process is important to mitigate this risk and to ensure that regulated services abide with duties under the Equality Act 2010 ('the EA 2010') which prohibits discrimination against persons sharing protected characteristics (including race, age, disability, sex, and gender assignment).[38]

---

[36] Further examples and information on checking that evidence is genuine or valid can be found in GPG45.
[37] The technical criterion of fairness is distinct from the principle of fairness in the UK General Data Protection Regulation (GDPR) which concerns how a user's personal data is processed. For more information, see ICO, *Principle (a): Lawfulness, fairness and transparency* [last accessed 23 November 2023] and ICO, 2023, Guidance on AI and data protection [last accessed 23 November 2023]
[38] Section 4 of the EA 2010.

How can service providers have regard to fairness when implementing age assurance?

Ensure the technology has been tested on diverse datasets

4.67 Fairness as a criterion applies when the age assurance method produces discriminatory outcomes that make it less effective for certain groups of users due to the internal functioning of the method. This applies in particular to age assurance methods which rely on machine learning or statistical modelling, as such bias may occur when the datasets used to train an algorithm are not sufficiently diverse. We expect service providers to ensure that, where relevant, their age assurance methods have been trained on diverse datasets.

Additional principles for providers to consider

4.68 Once a service provider has selected an age assurance process in line with the criteria, and provided it has found that process to be highly effective at determining whether or not a particular user is a child, the provider should also consider whether the process is easy to use and works for all users. Failing to do so might unduly prevent adult users from accessing legal content.

4.69 Service providers should therefore also consider the principles below when implementing age assurance methods or processes to ensure that adult users are not unduly excluded from accessing legal content (the 'principles'). These principles are set out in the following table.

Figure 4.3: Summary table of the principles that services providers should consider to ensure the age assurance process is easy to use.

Principles	Practical steps to consider principles
Accessibility: the principle that age assurance should be easy to use and work for all users, regardless of their characteristics or whether they are members of a certain group.	Assess the potential impact that the chosen age assurance method(s) might have on users sharing protected characteristics. Consider offering a variety of age assurance methods. Design the user journey through the age assurance process to be accessible for a wide range of abilities.
Interoperability: the ability for technological systems to communicate with each other using common and standardised formats.	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.

Accessibility

What is accessibility?

4.70 Accessibility refers to the concept that age assurance should be easy to use and work effectively for all users, regardless of their characteristics or whether they are members of a certain group.

Why is accessibility important?

4.71 If age assurance is not accessible to all users, it may unduly exclude some adults from accessing legal content. An inaccessible age assurance process might be one which is too difficult to use, leading users to abandon the process. Alternatively, the requirements of an age assurance process might make it inaccessible to certain groups of users, thereby excluding them from the process.

How can service providers have regard to accessibility when implementing age assurance?

Assess the potential impact that age assurance might have on different groups

4.72 All users are different. Before implementing the chosen age assurance method(s), service providers should therefore consider the potential impact that it might have on users with different characteristics.

4.73 This will assist providers in understanding the impact the chosen age assurance method(s) might have on different groups and whether it may be appropriate. It should also help providers to understand whether a particular age assurance method(s) may discriminate against or adversely impact particular groups, and to consider whether any adverse impacts on particular groups can be mitigated, for instance through the further steps outlined below.

4.74 Importantly, all users share multiple characteristics and the application of the chosen age assurance method(s) may be affected by the intersection of these characteristics. It is therefore important to consider impacts on a more holistic or cumulative basis (see 4.75(b) below).

4.75 In carrying out this assessment, providers may find it helpful to:

a) Consider potential impacts on users with “protected characteristics” under equalities legislation (including age, disability, gender reassignment, race, and sex, as well as users of different nationalities that may speak different languages).
b) Challenge themselves to think as broadly as possible, including indirect or cumulative impacts (intersectionality). For example, you may not consider that a particular age assurance method will discriminate against or adversely affect users of a particular race but it is possible that this assessment may change when, for example, you think about users of that race that are also of a particular sex and/or within a particular age bracket (specifically in this case, under or above 18).
c) Consider collecting evidence to properly assess potential impacts on particular groups e.g., through focus groups, surveys or reaching out to representative bodies, charities or communities.
d) Continually consider and review potential impacts and, where appropriate, revise the assessment as thinking progresses.
e) Record the assessment of potential impacts and mitigating steps so that it is clear how they determined what would be the most appropriate age assurance process for the service.

Consider offering a variety of age assurance methods

4.76 Some users may be unable, or may find it more difficult, to use certain kinds of age assurance methods. For example, those without credit cards will be unable to complete a credit card check. Those without a driving licence or passport will be unable to undergo a photo-ID check that relies on these documents.

4.77 Including multiple kinds of highly effective age assurance and allowing the user to choose which is most appropriate to them, is one means of helping to ensure that the overall age assurance process is accessible to users, regardless of whether they have certain characteristics or whether they are members of a certain group. However, service providers are not required to implement multiple kinds of age assurance and may be able to achieve an appropriately accessible age assurance process through a single age assurance method.

Design the user journey to be accessible for a wide range of abilities

4.78 There are many actions that service providers can take to make the user journey through the age assurance process easier to use and therefore more accessible.

4.79 This might include, for instance, ensuring that users with visual impairments are able to use screen readers to complete the age assurance process, or ensuring that all functionality is available from a keyboard for users with limited motor control.

4.80 The Web Accessibility Initiative's Web Content Accessibility Guidelines provide recommendations for how service providers can make content more accessible to users with a wide range of disabilities, including blindness, deafness, limited movement, and learning disabilities.

Interoperability

What is interoperability?

4.81 Interoperability describes the ability for technological systems to communicate with each other using common and standardised formats. It relies on consistent technological approaches being adopted across different methods. Standards, technical frameworks and other specifications are important to achieving interoperability.

4.82 In the context of age assurance, interoperability may involve re-using the result of an age check across multiple services allowing different providers of age assurance methods to share the information in line with data protection laws.

Why is interoperability important?

4.83 The principle of interoperability is useful for reducing the burden on the user as it limits the amount of information that users need to provide when accessing a new service if they have already proved their age elsewhere. This is a potential benefit to the user experience, as it reduces the time and effort required by users to understand, and input into, different age assurance processes. Providing less additional data in turn could reduce the data protection risks that might otherwise occur.

How can regulated services have regard to interoperability?

Stay up to date with developments in interoperability

4.84 The development of interoperable solutions for age assurance is still at an early stage, though there are several ongoing efforts to advance this. Given the benefits of interoperability discussed above, we encourage service providers to keep abreast of

developments in this area, and to consider implementing interoperable solutions to age assurance where they exist and are appropriate for the service.

4.85 Current efforts at enabling interoperable age assurance include:

a) The UK Government's Digital Identity and Attributes Trust Framework (DIATF) may enable interoperability between providers of digital identity and attribute services by encouraging the consistent adoption of common rules and standards. Certain digital identity and attribute services may provide or specialise in age assurance methods. The DIATF will come into full effect once the Data Protection and Digital Information Bill receives Royal Assent.

b) The euCONSENT project is a non-profit non-governmental organisation that has been established with the intention of designing, testing, and implementing extensions to the eIDAS infrastructure to enable open-system, secure and certified interoperable age verification.

c) The Open Wallet Foundation (OWF) is a consortium of companies and non-profit organisations collaborating to drive the global adoption of open, secure and interoperable digital wallet solutions.

Illustrative case study

4.86 In the table below, we provide an illustrative case study to explain how the criteria and principles set out in this section of the guidance might apply to an age assurance process.

4.87 Many alternative approaches to age assurance exist, and different approaches may be more suitable for different services. The below example is intended solely to illustrate how the criteria apply to assist service providers in complying with their duties relating to age assurance. This example should not be read as endorsing one particular age assurance method or process, nor should it be read as determinative that the given approach would be highly effective. Providers should decide what is the most appropriate method/process for their regulated service to ensure that children are not normally able to encounter pornographic content. Adhering to the process highlighted below is in no way determinative of compliance with the Part 5 duties – service providers need to be able to demonstrate that, as a result, children are not normally able to access pornographic content in their services.

Figure 4.4: An illustrative case study of how the criteria and principles might be applied to the age assurance process.

High-Level User Journey	Service provider considerations
(1) On accessing the regulated pornography service, a pop-up asks the user to confirm their age.	The service provider has ensured content is not visible prior to verifying the age of the user, to ensure children are not normally able to encounter pornographic content. It designs a pop-up box for the age assurance process that appears as a new, smaller window overlayed on top of the webpage that the user is viewing.
(2) The pop-up contains: **(a) Information on all the kinds of age assurance**	The service provider has set out a publicly available statement for its users explaining its age assurance process, as required by section 81(5) of the Act. Including this

High-Level User Journey	Service provider considerations
used, and how the processes work, in accessible language; **(b) A link to more detailed information, including relevant transparency information as per the requirements in the UK General Data Protection Regulation (UK GDPR);** **(c) A box reading "Understood – continue to age assurance."**	statement, or access to this statement, in the age assurance pop-up ensures that users can read the summary prior to the age assurance check, as outlined in paragraph 5.28 of this guidance.
(3) The user is directed to an age estimation check. At the bottom of the screen, the user can click on a link reading "prove my age another way." **During the age estimation process, the user is prompted to take steps to ensure the age estimation works effectively (e.g., ensure the lighting is appropriate).** **If the age estimation method estimates that the user's age is over a certain age, they are granted access to the site without further requirements.**	The service provider chooses an age estimation method and carries out the following checks against Ofcom's criteria. The estimation method could be purchased from a third-party vendor or developed internally but the platform must ensure in either case the relevant checks are carried out to assess if the method is highly effective. • Technical accuracy – The service provider assesses the results of performance testing of the age estimation method and determines that the level of technical accuracy is not high enough for users with an age close to 18, and a challenge age is needed. The service provider adds a secondary method to the age assurance process as described in the next section of this table. • Robustness – The service provider carries out real-world testing to ensure that the estimation method performs to a suitable level in practice. It also determines that the method is not susceptible to any circumvention techniques that are easily accessible to children – for example, it uses presence detection. • Reliability – The service provider repeats the testing undertaken in the steps above. It selects a timeframe to conduct this testing that is derived from their risk assessment process. Additionally, it closely monitors the ongoing performance and outputs of the method by, for example, noting any trends of inaccurate age estimations and/or a rise in complaints/appeals. Undertaking additional subsequent testing, monitoring performance and taking necessary remedial action promptly, should

High-Level User Journey	Service provider considerations
	ensure that the service provider maintains the initial performance it observed. • Fairness – The service provider ensured that during development of the solution, steps were taken to train the model on a diverse dataset. When considering test results, it ensures that performance across different protected characteristics has minimal variations.
(4) If the age estimation method determines that the user's age is lower than the challenge age, then the user must undergo an age verification check.	The service provider, having assessed that the estimation method is not sufficiently technically accurate for users whose age is close to 18, decides to choose an age verification method for those users. The verification method could be purchased from a third-party vendor or developed internally, but the platform should ensure the relevant checks are carried out to assess if the method is highly effective. • Technical accuracy – The service provider assesses the results of performance testing of potential age verification methods and chooses one (or more) that provide(s) a high level of technical accuracy. • Robustness – The service provider chooses a verification method that sufficiently guards against fake input and sufficiently binds the proof of age to the user presenting for the age check. • Reliability – The service provider takes steps to ensure that the chosen secondary age assurance method performs consistently. For example, this may mean ensuring that the method can identify new or updated identification documents, or identification documents from non-UK territories. It also means, as with the solution above, that periodic testing is undertaken to ensure consistent performance. • Fairness – The service provider undertakes an assessment to ensure that the method performs to an equivalent level of accuracy for users with different characteristics. Once the service provider has determined that its age assurance process as a whole is highly effective, it then considers the guidance principles to ensure the process is easy to use and does not unduly exclude adult users: • Accessibility – The service provider considers the impact of the age assurance process on users with different characteristics. While it considers that having a secondary method mitigates the potential negative impact for young adults who look younger

High-Level User Journey	Service provider considerations
	than 18 if relying on facial age estimation, it identifies that the overall user journey may be difficult to use for users with disabilities. It consults the Web Content Accessibility Guidelines and implements relevant measures to make the age assurance process easier to use, such as reducing the complexity of the text guiding users through the age checks by shortening sentences and using bulleted lists where appropriate. • In addition, the provider carries out an assessment to understand the proportion of users who would likely possess the necessary proof to verify their age and whether implementing this method would cause a disproportionate number of specific users to be excluded. The service provider decides that that a large volume of users could verify their age in this way with minimal negative impact. • Interoperability – The service provider looks into the current efforts to enable interoperable age assurance. It identifies a project that may be appropriate for its service and may help to reduce the potential burden on users. The provider decides to regularly review the project status to determine if is ready to implement.
(5) If the age estimation method determines that the user's age is equal to or higher than the challenge age, or if the age verification method determines that the user's age is 18 or above, the user's access to pornographic content is enabled. Otherwise, the provider denies the user who has failed the relevant age check access to any part of the service that hosts regulated provider pornographic content.	The service provider continues to monitor the performance of both methods in multiple ways and ensures that it takes action if any of them fall below being highly effective.

5. Duties to keep a written record

The record-keeping duties

5.1 The Act sets out the following duties relating to record-keeping:

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; [39] 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), [40] 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 about which kinds of age verification or age estimation a service provider is using and how they are used. [41]

5.2 Throughout this guidance, we refer to the duties described in paragraph 5.1 as the **'record-keeping duties.'**

5.3 These requirements can be broken down into the following core elements:

i) The service provider keeps a written record of the type or types of age assurance it uses and how it does so;

ii) The service provider keeps a written record of how it has considered privacy and data protection laws when making a decision as to how it will use age assurance;

iii) The service provider produces a summary of the parts of the written record that relate to how it has complied with the duty set out in section 81(2) of the Act;

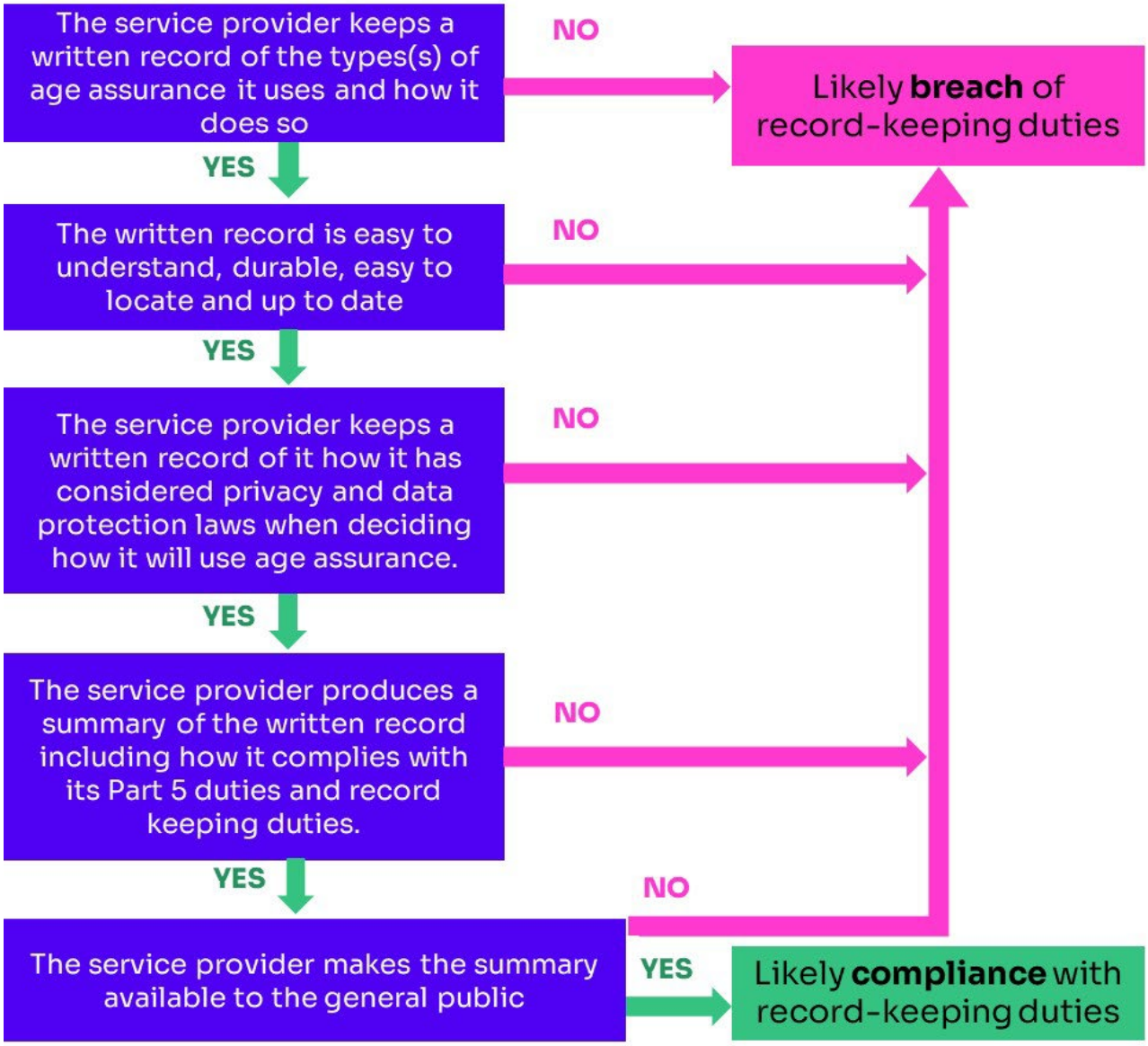
iv) The summary in question includes details of the types of age assurance the service provider uses and how it does so; and,

v) The summary is available to the general public.

5.4 The following diagram provides an overview of the analytical framework Ofcom will use to assess compliance with these duties.

[39] Section 81(4)(a) of the Act
[40] Section 81(4)(b) of the Act.
[41] Section 81(5) of the Act.

Figure 5.1: Analytical framework for assessing in scope services' compliance with the record-keeping duties.



5.5 This section provides guidance to assist service providers in complying with each of these elements. As well as guidance on how to keep a written record effectively, it covers what to include in a written record of the kinds of age assurance used and how they are used, and in a written record of having regard to user privacy. In addition, we provide guidance on making a publicly available statement. We also set out examples of circumstances where we are likely to consider that a service provider has not complied with its record keeping duties.

How to keep a written record

5.6 The written record which a service provider keeps of the age assurance process it uses must be easy to understand, and additionally, should be durable, easy to locate, and up to date.

5.7 Written records can be made and kept in a durable medium of the service provider's choice (for example, on a computer or using any storage device such as a CD-ROM, USB memory stick, cloud storage, a network drive or a paper copy), which is capable of being provided easily and quickly to Ofcom if required.

5.8 Written records should be legible and written in as simple and clear language as possible. They should not include jargon, encryption, shorthand or code such that Ofcom cannot understand what they say.

5.9 Where reasonably practicable, written records should be kept in English (or for service providers based in Wales, in English or Welsh).

Example of non-compliance

The written record is written in an incomprehensible format that means it cannot be easily understood by Ofcom.

5.10 The service provider must keep a written record of the current age assurance process that it deploys to comply with the age assurance duties. Providers should make the record as soon as possible after the deployment of any new method and keep it updated to ensure it remains current. It is important that earlier versions of the record are retained so that the provider can provide both current and historic records of how it has complied with the age assurance duty.

Example of non-compliance

The service provider has not updated its written record to ensure it remains current.

5.11 Written records should be dated for when they are made and on each occasion that they are updated.

5.12 Service providers should retain written records in accordance with their record retention policies, or a minimum of five years (either calendar or financial), whichever is the longer, even though there may have been subsequent revisions to reflect changes to the service provider's compliance measures. This will ensure that the provider is able to provide both current and historic records of how it has complied with the relevant duties.

On the kinds of age assurance used and how they are used

5.13 When making and keeping a record of the kinds of age assurance used, and how they have used them, service providers should detail:

i) Any third-party supplier contracted to provide an age assurance process;
ii) What kind of age assurance the process uses (whether consisting of one or multiple methods).

5.14 We expect service providers to include in their written record how each method or combination of methods fulfils the criteria and principles set out in Section 4. In Section 4, we have set out ways in which providers can have regard to the criteria and principles when implementing age assurance.

Example of non-compliance

The service provider has not described, in its written record, the kinds of age assurance method(s) it uses, or how they are used, to ensure that children are not normally able to encounter regulated provider pornographic content on its regulated service(s).

On having regard to privacy and data protection

5.15 For an understanding of how to have regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy, service providers should familiarise themselves with the data protection legislation, and how to apply it to their age assurance method, by consulting ICO guidance.

The Data Protection Regime

5.16 The UK data protection regime is made up of several pieces of legislation, including the Data Protection Act (DPA) 2018, the UK GDPR, and the Privacy and Electronic Communications Regulations (PECR) 2003. Taking data protection requirements into account will help service providers to meet the record-keeping duty related to privacy set out at paragraph 5.1(ii).

5.17 Together, this legislation provides a risk-based framework for making sure the processing of personal data respects the fundamental rights and freedom of individuals. The ICO is responsible for upholding information rights through its oversight and enforcement of the legislation.

5.18 Service providers should consult ICO guidance 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.[42]

5.19 The PECR will apply to anyone who stores information on or gains access to information on a user's device, for example, by using cookies or other similar technologies. The ICO has produced detailed guidance on this topic.

ICO guidance on data protection and age assurance

5.20 The data protection principles are the cornerstone of the UK GDPR.[43] They apply whenever services process personal data, including for the purposes of age assurance. The principles are:

a) Lawfulness, fairness and transparency[44]
b) Purpose limitation[45]
c) Data minimisation[46]
d) Accuracy[47]
e) Storage limitation[48]
f) Security[49]

5.21 Accountability is the seventh principle. It requires organisations to demonstrate compliance with data protection legislation.[50]

---

[42] ICO, 2023, A guide to the data protection principles [accessed 23 November 2023]; ICO, A guide to lawful basis [accessed 23 November 2023]; and ICO, Individual rights – guidance and resources [accessed 23 November 2023].
[43] For an overview of each principle, see the ICO's guide to the data protection principles.
[44] ICO, Principle (a): Lawfulness, fairness and transparency. [accessed 23 November 2023].
[45] ICO, Principle (b): Purpose limitation. [accessed 23 November 2023].
[46] ICO, Principle (c): Data minimisation. [accessed 23 November].
[47] ICO, Principle (d): Accuracy. [accessed 23 November 2023].
[48] ICO, Principle (e): Storage limitation. [accessed 23 November 2023].
[49] ICO, Principle (f): Integrity and confidentiality (security). [accessed 23 November 2023].
[50] ICO, Accountability and governance. [accessed 23 November 2023].

5.22 Before compiling a written record for the purposes of compliance with the duties set out in the Act, service providers should familiarise themselves with the Commissioner's Opinion on Age Assurance for the Children's code ('the Opinion'), which outlines how the data protection principles and other requirements can be considered in the context of age assurance. The considerations set out in the Opinion are technology neutral, making them applicable to any kind of age assurance. [51]

5.23 Consulting the Opinion will help service providers implement age assurance while protecting user privacy in line with the data protection regime. This will help service providers to keep a written record of how they have regard to the importance of protecting UK users from a breach of any statutory provision or rule of law concerning privacy.

Examples of how to keep a written record regarding protecting user privacy

5.24 When considering compliance, Ofcom will consider whether service providers have kept a written record of how they have had regard to privacy and data protection requirements in making decisions around age assurance. Where we have concerns that a provider, based on its written record, has not complied with its obligations under data protection laws, we may refer the matter to the ICO.

5.25 The examples listed below are ways to demonstrate compliance with data protection law, which can also help service providers to comply with the written record duty in relation to privacy under the Act.

a) **Conducting a Data Protection Impact Assessment (DPIA).** These are required by data protection law where processing is likely to result in a high risk to the rights and freedoms of individuals. DPIAs will assist service providers in identifying and mitigating the risks arising from their processing of personal data, which can help demonstrate that they have had regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy. ICO guidance states that providers should identify and assess risks, and identify options for reducing said risks. Detailed guidance on how to carry out a DPIA, and a sample template, can be found on the ICO website.

b) **Providing privacy information to users.** Service providers should give users information about why they need to provide any personal data, how it will be processed, how long it will be retained, and if it will be shared with anyone else. More information on privacy notices can be found on the ICO website.[52]

c) **Keeping written records of processing activities.** Most organisations that process personal data must document their processing activities to some extent.[53]

d) **Having up to date data protection policies along with a record of how providers make staff aware of them.** This provides staff with clarity and consistency around their data protection obligations.[54]

e) **Having a record of which staff have completed any data protection training programme that is in place.** This helps to ensure all staff have adequate knowledge of data protection, as appropriate for their role.[55]

---

[51] See ICO, Children's code guidance and resources for the Commissioner's Opinion on Age Assurance.
[52] See ICO, Transparency (cookies and privacy notices), and ICO, How to write a privacy notice and what goes in it.
[53] ICO, Records of processing and lawful basis. [accessed 23 November 2023].
[54] ICO, Policies and procedures. [accessed 23 November 2023].
[55] ICO, Training and awareness. [accessed 23 November 2023].

f) **Clearly documenting technical and organisational security measures.**[56]

Example of non-compliance

There is no mention of how the service provider has had regard to the importance of protecting the privacy of UK users in its written record.

Making a publicly available statement

5.26 The Act requires service providers to set out in a publicly available statement a summary of the kind(s) of age assurance used and how they have used it, as described in their written record. The Act defines 'publicly available' as "available to members of the public in the UK."[57]

5.27 In summarising the written record, the service provider should aim to provide the main details about the age assurance process which it uses. This will help to explain to users of the regulated service what the process is designed to do and how it works, so that users can understand why it is necessary and how to complete the process. This will also support the accessibility principle. In addition, the provider should omit any information which is commercially sensitive. We also recommend providers to identify and omit from the summary any information which might pose a security risk to the service or other relevant parties, or any information which might expose the age assurance process to increased risk of circumvention, if made available to the public.

5.28 Service providers should ensure that the statement is available to members of the UK general public in an easy to find area of the regulated service that is clearly labelled and accessible to users from the point that they first access the service. For instance, the section at the top (header) or bottom (footer) of the webpage, where users can typically find site contact details and navigation links. The header and footer are generally displayed on every page of the website, so are easily accessible. To ensure that users can read the summary prior to completing the age assurance check, providers should include the summary alongside any explanatory text on how the age assurance process works. This could be in the form of a pop-up, for example, a smaller, new window that appears overlayed on top of the webpage, drawing the user's attention. The summary text could be included in this window, or the pop-up could feature a button prompting users to click for more information.

5.29 Service providers should write the statement in accessible language that is formatted in a way that helps the public to understand the kinds of age assurance used and how they have been used.

5.30 Service providers should design the statement for the purposes of ensuring usability for users with disabilities who rely on assistive technologies to use the internet. [58] For example:

a) ensuring that all functionality for accessing the statement is available from a keyboard, to allow users with limited fine motor control to use keyboard navigation technology instead; or,

---

[56] ICO, A guide to data security. [accessed 23 November 2023].
[57] See section 236 of the Act.
[58] The Assistive Technology Industry Association (ATIA) defines assistive technology as "any item, piece of equipment, software program, or product system that is used to increase, maintain, or improve the functional capabilities of persons with disabilities" ATIA, What is AT? [accessed 17 November 2023].

b) providing alternative text for any images used within the statement to allow users with visual impairments to use a screen reader, which reads aloud the information on the page.[59]

Example of non-compliance

The service provider has not summarised its written record in a publicly available statement, or the statement is not available to users.

[59] Web Accessibility Initiative, 2022, Introduction to Web Accessibility. [accessed 23 November 2023].

6. Assessing compliance with age assurance and record-keeping duties

6.1 In this section, 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. We also set out where providers can find further information on Ofcom's enforcement processes relating to the Act.

6.2 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.[60] Sections 4 and 5 of this guidance provide the analytical frameworks Ofcom intends 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.

6.3 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.[61]

6.4 Our Online Safety Enforcement Guidance ('OS Enforcement Guidance') sets out the procedures we will follow where we suspect non-compliance with the obligations that apply to service providers under the Act.[62] It also outlines the different enforcement tools that we may use and explains how we prioritise cases that come to our attention, according to:

a) the risk of harm or seriousness of the alleged conduct and any impact this may have on the risk of harm presented by content available on the regulated service;[63]
b) the strategic significance of addressing the conduct; and
c) the resource implications and risks in taking enforcement action.

6.5 Section 3(4A) of the CA03 requires us to have regard to, among other matters, the need for a higher level of protection for children than for adults.[64] Section 151(3) of the Act also states that our enforcement guidance must include an explanation of how we will take account of the impact (or possible impact) of non-compliance on children.

6.6 We will include the harm or risk of harm to children in our prioritisation framework when considering:

a) the risk of harm or seriousness of the conduct; and

[60] Schedule 13 paragraph 4 of the Act.
[61] Section 3(3)(a) of the CA03.
[62] The OS Enforcement Guidance is currently in draft form and subject to consultation. Accordingly, this link will be updated in due course once the OS Enforcement Guidance is finalised and published.
[63] In this context, seriousness includes whether the conduct is, or appears to be "a repeated, intentional, systemic, or particularly flagrant contravention."
[64] As amended by the Act. Section 3(h) of the CA03 also requires us to have regard to the vulnerability of children in performing our duties.

b) the strategic significance of addressing the alleged contravention.

6.7 Including the risk of harm to children in two parts of Ofcom's prioritisation framework reflects the importance of this factor in considering whether or not to take enforcement action.

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

A1. Glossary

Technical glossary

Metrics used to measure the accuracy of age assurance

Term	Meaning
True positives (TP)	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.
False positives (FP)	For the purpose of age assurance, this refers to an outcome where a model incorrectly predicts a positive class i.e., a user is 18 or over and the model predicts their age as under 18.
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.
Accuracy (ACC)	The fraction of the predictions the model got right. The formula is ACC = (TP + TN) / (TP+ TN + FP + FN).
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).
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).
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).
Error	The user's age determined by the technology minus the user's actual age. An overestimation yields a positive value, whereas an underestimation yields a negative value.
Absolute error (AE)	The same as the 'error,' but disregards the sign (i.e., positive or negative) thus focusing only on the magnitude (size) of the difference between the technologically-determined age and actual age.

Term	Meaning
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.
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.
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.
Cumulative score (CS)	An aggregated score that is calculated by summing the individual score across over a period of time/category etc.

Terms used in this guidance

Statutory definitions

Term	Meaning
'Age estimation'	"Any measure designed to estimate the age or age-range of users of a regulated service."[65]
'Age verification'	"Any measure designed to verify the exact age of users of a regulated service."[66]
'Child'	"A person under the age of 18."[67]
'Provider'	"The entity that has control over which content is published or displayed on the service."

[65] Section 230(3) of the Act.
[66] Section 230(2) of the Act.
[67] Section 236(1) of the Act.

Term	Meaning
	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."[68] "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."[69]
'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."[70]
'Regulated provider pornographic content'	Provider pornographic content other than content that – i) "Consists only of text, or ii) 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),[71] or iii) "Consists of a paid-for advertisement."[72]
'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;

[68]Section 226(8)-(9) of the Act.
[69] Section 226 (10)-(11) of the Act.
[70] Section 79(2) of the Act.
[71] Section 79(4) of the Act.
[72] Section 79(5) of the Act.

Term	Meaning
	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.)"[73] It does not include pornographic content that - d) "appears in search results of a search service or a combined service,"[74] or e) "is user-generated content in relation to that service."[75]
'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."[76]

Additional terms used in this guidance

Term	Meaning
Age assurance	Refers to both age verification and age estimation, as defined in section 230 of the Act. For these purposes, self-declaration of age is not considered to be a form of age assurance.
Age assurance method	Refers to the particular system or technology that underpins an age assurance process.
Age assurance process	Refers to 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.

[73] Section 79(6)(a) of the Act.
[74] Section 79(6)(b) of the Act.
[75] Section 79(7) of the Act.
[76] Section 55(3) of the Act.