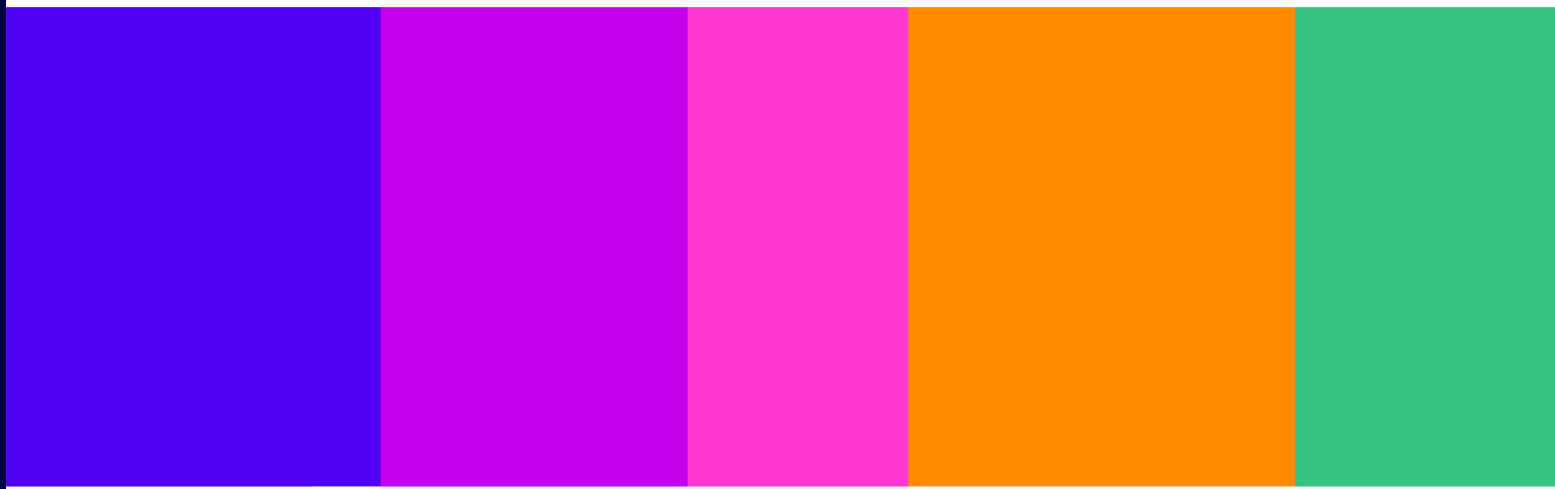


Volume 5

Annexes

Statement

Published 24 April 2025



Contents

Annex

| | |
|---|----|
| A3. Further detail on economic assumptions and analysis..... | 3 |
| A4. Legal framework: Duties of providers and Ofcom in relation to the protection of children | 14 |
| A5. Equality Impact Assessment and Welsh Language Assessment | 43 |
| A6. Additional measures suggested by stakeholders..... | 57 |
| A7. Glossary | 69 |

A3. Further detail on economic assumptions and analysis

- A3.1 This annex provides further information related to the economic analysis used to support our provisional conclusions for some of the measures assessed in this Statement. We outline:
- a) General assumptions we have used to develop quantified cost estimates across several of the measures; and
 - b) More detail on specific assumptions and analysis related to Age Assurance.

General cost assumptions

- A3.2 We have made some general assumptions on costs, which apply to our analysis of many of the measures. These general assumptions are usually combined with other assumptions that are specific to each measure to determine the estimated costs of measure in the chapters in the main body of the report. Any additional assumptions that are used in the cost analysis are described in the costs section of the relevant chapters.

Price Level

- A3.3 All quantified estimates of costs are provided in 2023 prices, unless otherwise stated. We have used 2023 prices, as that is the year of the most recent final Annual Survey of Hours and Earnings ('ASHE'), which we use to develop estimates for the labour cost required to implement some code measures.¹
- A3.4 Our Illegal Harms Statement, which includes cost analysis for some similar measures in the current statement, also used 2023 ASHE data.

Labour Costs

- A3.5 To develop estimates for labour costs, we have used the ASHE 2023 gross median full-time earnings for the four occupations listed below. These occupations are likely to develop and/or manage the systems and processes that in-scope services will need to have to comply with the regime.²
- A3.6 The four professions we have determined to be most relevant for the measures, and their relevant Standard Occupational Classification ('SOC') 2020 references are as follows:
- a) Programmers and software development professionals' salary (2134) to estimate the cost of 'software engineer' time used when developing our cost estimates.

¹ Office for National Statistics ('ONS'), 2023. [ASHE, Table 14, 2023 revised estimates](#). We acknowledge that ASHE data for 2024 has been released, although that data is still provisional at the time of writing. We consider that our approach to quantification, including use of a 2023 price level, is adequate for assessing the likely impacts of the measures, taking into account how we apply salary assumptions to reflect the possibility that actual salaries may be higher than suggested by the ASHE data, as explained in the next section below.

² ASHE documentation does not explicitly state that gross salaries include bonuses, but our understanding is that the gross pay includes bonuses, tips and other payments.

- b) Database administrators and web content technicians (3133)³ salary to estimate the cost of ‘content moderator’ time used when developing our cost estimates.
 - c) Professional Occupations (2) to cover a range of professions that are employed at various online services and might be required to implement code measures. This could be legal employees, operations, product managers and so forth.
 - d) Graphic and multimedia designers’ salary (2142) to estimate the cost of ‘Graphic and multimedia designer’ time used for creating audio-visual support materials.
- A3.7 We recognise that for some service providers, median UK wage rates may differ from actual salary rates. This may be especially the case for larger service providers based in the US, who may have higher salary levels. We also appreciate that the salary costs of some types of staff, such as software engineers with certain specialisms, may vary and may be considerably higher in some cases. To take account of this, we also use a higher salary estimate, which is double the value of our lower estimate.
- A3.8 Conversely, some service providers may outsource some relevant work to locations where average pay is lower than the UK, which may reduce these costs. To the extent this is the case, our salary range may tend to overstate costs.
- A3.9 We applied a 22% uplift to the gross wage costs to account for non-wage labour costs, such as employers’ National Insurance contributions.⁴
- A3.10 Table A1.1 shows the ‘low’ and ‘high’ labour cost estimates for different time periods, including the 22% uplift, for each of the four occupations which is based on annual labour costs with a calculation methodology applied to derive monthly and weekly estimates.⁵

³ This four-digit SOC 2020 code (unit group code 3133) includes occupations such as content, chat, web, and website moderators as well as other occupations such as database administrators and web content technicians. ONS, [SOC 2020 Volume 2: the coding index and coding rules and conventions](#) [accessed 25 March 2024]. The associated ONS spreadsheet can be found here: [SOC 2020 Volume 2: the coding index](#).

⁴ This is the non-wage uplift recommended by the Regulatory Policy Committee (‘RPC’). Source: RPC, 2019. [RPC guidance note on ‘implementation costs’](#). It is also the uplift used by DSIT in its Impact Assessment for the Online Safety Act. Source: DSIT, 2024. [Online Safety Act impact assessment](#), paragraph 132 [accessed 7 January 2025]

⁵ When producing cost estimates for the measures, we have used resourcing estimates based on different time periods (e.g. days/weeks/months) suitable for the particular measure. The annual wages are derived from the Office for National Statistics (‘ONS’), 2023. [ASHE, Table 14.7a Gross annual pay for full-time employees, 2023 revised estimates](#). The monthly wages are derived from dividing the annual wages by the number of months in a year (12). The weekly wages are derived from the Office for National Statistics (‘ONS’), 2023. [ASHE, Table 14.1a Gross weekly pay for full-time employees, 2023 revised estimates](#). The daily wages are derived from dividing the annual wages by the number of working days in a year. We assume on average there are 228 working days in a year. This assumes people work 5 days a week and that there are 8 bank holidays and on average people take an additional 25 days leave a year. The hourly wages are derived from the Office for National Statistics (‘ONS’), 2023. [ASHE, Table 14.5a Gross hourly pay for full-time employees, 2023 revised estimates](#). [all accessed 28 January 2025]

Table A1.1: Low and High Range - Estimates of Labour Costs⁶

| Occupation | Low | High |
|---------------------------------|-------------------------------|----------|
| | Annual labour cost estimates | |
| Software engineer | £60,305 | £120,609 |
| Content moderator | £38,430 | £76,860 |
| Professional occupations | £52,693 | £105,386 |
| Graphic and multimedia designer | £35,507 | £71,014 |
| | Monthly labour cost estimates | |
| Software engineer | £5,025 | £10,051 |
| Content moderator | £3,203 | £6,405 |
| Professional occupations | £4,391 | £8,782 |
| Graphic and multimedia designer | £2,959 | £5,918 |
| | Weekly labour cost estimates | |
| Software engineer | £1,177 | £2,354 |
| Content moderator | £736 | £1,472 |
| Professional occupations | £1,047 | £2,093 |
| Graphic and multimedia designer | £696 | £1,393 |
| | Daily labour cost estimates | |
| Software engineer | £265 | £530 |
| Content moderator | £169 | £338 |
| Professional occupations | £231 | £463 |
| Graphic and multimedia designer | £156 | £312 |
| | Hourly labour cost estimates | |
| Software engineer | £31 | £63 |
| Content moderator | £20 | £39 |
| Professional occupations | £29 | £57 |
| Graphic and multimedia designer | £18 | £37 |

A3.11 For a few measures that require input from senior management, we have used salary estimates for additional occupations.⁷ These include senior managers or senior leaders

⁶ While the 'high' estimates have been derived from doubling the 'low' estimate, they may not match exactly due to rounding.

⁷ This is based on simple assumptions we have made of £100,000 salary for a senior manager and £150,000 salary for a senior leader, which are then uplifted by the 22% uplift for non-wage labour costs.

with an estimated annual labour cost of £122,000 to £183,000. These also include S&P 500 Independent Director with an estimated annual labour cost of £310,000 per year.⁸

Non-engineering Costs for System Changes

A3.12 Where system or other software changes associated with a measure involve a software cost, we typically match the amount of engineering time with an equivalent amount of non-engineering time for work carried out by people in professional occupations. This is to account for non-engineering labour time that a business might need to spend on a system change, for instance legal or project management associated with the change.

Maintenance Costs for System Changes

A3.13 Where system or other software changes associated with a measure involve an initial cost, we have assumed an ongoing annual maintenance cost of 25% of the initial cost. These ongoing costs reflect work likely required to ensure the system continues to operate as intended. We have applied this assumption in the absence of actual information about the ongoing maintenance costs. We did not receive any stakeholder feedback on this assumption in response to the consultation.

Further detail on age assurance cost analysis

A3.14 This sub-section provides further analysis of costs which has been used to support our conclusions on age assurance measures, as set out in section 13. We discuss:

- a) Our general cost assumptions for age assurance.
- b) Direct costs to service providers. We consider that all direct costs are likely to depend on how a service provider approaches its implementation of the measures, but in all cases we consider that the main costs are likely to relate to:
 - i) preparing to implement age assurance; and
 - ii) implementing and operating a third-party age assurance method; or
 - iii) building and operating an in-house age assurance method.
- c) Indirect costs to services due to our requirements to implement age assurance.

Our general cost assumptions for age assurance

A3.15 We adopt several general assumptions to estimate costs. The cost estimates are illustrative and may not capture the full range of possibilities in practice. Providers could face different costs depending on their circumstances (e.g. any existing age assurance capabilities), the age assurance method(s) they adopt and how they implement their age assurance process more broadly.

A3.16 We have assumed that users will have to confirm their age for each service separately. We recognise that where an online service provider manages multiple services it may be possible to share the age credential of a user across more than one service, which may reduce direct costs for the service and friction on users. Reusability of age checks and/or

⁸ The annual compensation for an S&P Independent Director is based on Spencer Stuart, [2023 S&P 500 Compensation Snapshot](#), converted to GBP, with additional assumption that such persons spend approximately 250 hours per year in their role based on [PwC's 2022 Annual Corporate Directors Survey](#). [all accessed 28 January 2025]. The resulting annual wage is £254,000 to which 22% uplift is applied for nonwage labour costs.

interoperability of age assurance methods may become more widely available in future, for example, where a user can complete an age check that is valid for many service providers. This could reduce costs and make implementing and operating age checks more cost effective for more services, and more convenient for users.

- A3.17 We have assumed that service providers have no existing systems in place that can facilitate age assurance. Where services already have systems to gate access for users in some way or to obtain user information that may be relevant for age assurance (e.g., a payment system for subscription charges), the costs of implementing age assurance may be lower than our estimates suggest. This includes cases where a service may also be subject to regulatory requirements related to age assurance in other jurisdictions.
- A3.18 We assume that age checks are one-off. As we set out in the Part 3 HEAA Guidance, we have not set specific expectations for service providers to repeat age checks. However, service providers should determine whether repeated age checks are needed to meet the robustness criterion based on the features of their service and age assurance process. For example, service providers may decide to conduct an age check each time an unregistered user visits a service. We note that services which do not offer accounts or where users do not choose to create accounts, could incur higher costs. Service may also face higher costs if users repeat the age check, e.g., children who repeat the age check after turning 18. However, we understand that some age assurance providers offer volume discounts to services⁹ which could reduce the overall costs of these age checks for services which have to repeat age checks for users.
- A3.19 We have assumed that services apply age assurance to all users. In practice, some services may be able to only age assure a subset of users. For example, as explained in age assurance Section 13, for Measures PCU B4 to PCU B7 a service may only conduct age checks for users who are seeking access to certain content harmful to children. Depending on the specific context of a service, this may significantly reduce costs compared to the estimates we present. For instance, if a service conducted age checks for 50% of its users, and its costs were primarily driven by unit costs per age check, then we would estimate its ongoing costs related to conducting age checks to be up to 50% lower.
- A3.20 We do not make specific assumptions in relation to challenge age. Our Code makes clear that providers using age estimation should use a challenge age approach, but the specific implications of this will depend on the age assurance process implemented in each case. When forming our view of likely costs per user (charged by third-party age assurance providers) we have taken into account that a minority of users may require a second age assurance method, which could entail additional costs. Our assessment of the costs of developing age assurance in-house discusses the development of a single age assurance method but we acknowledge that costs are likely to be significantly larger where multiple methods are developed and implemented.
- A3.21 We recognise that our cost estimates are dependent on the assumptions we have made. In practice costs could be higher or lower, depending on how service providers have decided to comply with their online safety duties and implement age assurance.

Preparatory costs relating to the introduction of age assurance

⁹ DSIT, 2024. [Online Safety Act impact assessment](#), paragraph 190 [accessed 7 January 2025].

- A3.22 All U2U services are likely to incur some one-off preparatory labour costs relating to the preparation of adopting age assurance. These may include staff familiarising themselves with the measures and guidance, familiarising themselves with ICO guidance, researching and assessing the suitability of different age assurance options for their service, considering how to implement age assurance in a way that is highly effective, meeting the relevant criteria and having regard to the other principles (such as accessibility).
- A3.23 Where a service provider decides to use a third-party age assurance provider, the procurement process is likely to involve some time and effort related to governance and budget processes, evaluation of providers and senior management engagement. For larger businesses with relatively complex governance and procurement processes, a formal tendering process could tie up internal staff's time and take significantly longer.
- A3.24 Overall, these preparatory costs are likely to depend on the size and type of service and are expected to be larger for large services because of different governance processes but also the number of employees likely to be involved.

Costs associated with third-party age assurance methods

- A3.25 There may be upfront costs linked to the age assurance provider setting up a client account to prepare the age assurance method for use, or in some cases, this charge may be part of an ongoing maintenance support service.¹⁰ We recognise that these upfront costs may be substantial for larger, more complex services, e.g. if the existing service infrastructure needs adjusting or there are other complexities with linking up the third-party technology with the services' systems or data. For instance, a report commissioned by DSIT found an example of a 'large gaming organisation' which received cost estimates from a third-party age assurance provider that it would incur '2-3 months of 4-5 developer's time' to implement the technology on its service.¹¹ However, our overall assessment is that this cost is likely to be small for most smaller services. For instance, we understand that some third-party methods are developed with ease of integration in mind, meaning that connecting to a services' existing systems should be relatively easy and cheap.
- A3.26 The service provider may have to also introduce access controls as part of implementing the Age Assurance measures and the related Content Moderation and Recommender System measures. For example, this may involve tagging users so that children can get a more age-appropriate experience or are prevented from accessing parts of the services not suited for them. This may require changes to the existing ICT infrastructure or building of a new user interface to integrate age assurance with the service, which could mean costs could be material, although requirements and costs are likely to vary by service and approach to implementation.
- A3.27 The service provider may also need to train some of its staff who work closely with the age assurance process (e.g., software engineers maintaining the running of the age assurance software) when the process becomes operational. We expect such costs would be relatively small and could be larger in an alternative approach where age assurance technology is developed and implemented fully in-house.

¹⁰ For example, based on Yoti's price list data from May 2022, setting up an organisational account is £750 per organisation. [GC-13 Yoti Age Verification Pricing \(digitalmarketplace.service.gov.uk\)](https://digitalmarketplace.service.gov.uk) [accessed 23 February 2024].

¹¹ DSIT, 2024. [Potential impact of the Online Safety Bill](#) [accessed 27 January 2025].

- A3.28 The main cost component relating to third-party age assurance methods is the per-check cost, including the cost to check the age of existing users and new users on an ongoing basis. These costs are likely to vary depending on the age assurance process and provider, as underlying costs and pricing approaches vary. According to DSIT's impact assessment of the Online Safety Act, some age assurance providers offer volume discounts to services requiring a large number of checks and discounted fees for small clients and start-ups in some cases,¹² while subscription-based verification packages often include a fixed number of checks for users.¹³ DSIT's evidence indicates that price per check ranges from less than 1p to £1, depending on the provider and method used.¹⁴
- A3.29 To illustrate what these costs may mean for a service, we set out cost examples for hypothetical services with a different number of users in the table below. According to the Government's impact assessment on the Online Safety Act, most per-check costs provided were 10p or lower.¹⁵ We have also reviewed evidence from consultation responses and other relevant considerations, as discussed in Section 13. Our approach reflects the variety of methods and prices available in the market, as well as uncertainty about how the market may evolve in future.
- A3.30 We use a low estimate of 5p per check and a high estimate of 30p. Considering the prevalence of volume discounts, we expect a smaller service is more likely than a larger service to incur per-check costs closer to the high estimate. However, this is partly mitigated by large services being likely to face more substantial preparatory costs or requiring a significantly higher volume of age checks.

¹² DSIT, 2024. [Online Safety Act impact assessment](#), paragraph 190 [accessed 7 January 2025].

¹³ DSIT, 2024. [Online Safety Act impact assessment](#), paragraph 186 [accessed 7 January 2025].

¹⁴ It is possible that due to inflation that these examples are now out of date. Publicly available per check prices are greater than the bottom end of this range, and in these cases, it is not clear who these prices would apply to. DSIT, 2022. DSIT, 2024. [Online Safety Act impact assessment](#), paragraph 190 [accessed 7 January 2025].

¹⁵ DSIT, 2024. [Online Safety Act impact assessment](#), paragraph 190 [accessed 7 January 2025].

Table A1.5: Illustrative cost estimates of age checks via third-party age assurance providers*

| Existing UK user base | New users each year | Age assurance for existing users | Age assurance for new users (annual ongoing cost) |
|-----------------------|---------------------|----------------------------------|---|
| 100,000 | 10,000 | £5,000 - £30,000 | £1,000 - £3,000 |
| 350,000 | 35,000 | £18,000 - £105,000 | £2,000 - £11,000 |
| 700,000 | 35,000 | £35,000 - £210,000 | £2,000 - £11,000 |
| 1,000,000 | 50,000 | £50,000 - £300,000 | £3,000 - £15,000 |
| 7,000,000 | 70,000 | £350,000 - £2,100,000 | £4,000 - £21,000 |
| 20,000,000 | 200,000 | £1,000,000 - £6,000,000 | £10,000 - £60,000 |

Source: Ofcom analysis

**Note: All cost estimates have been rounded up to the nearest thousand. These illustrative examples assume a faster rate of user base growth, in proportionate terms, for the smallest services (10% growth rate) and a lower rate for the largest services (1% growth rate).*

- A3.31 We assume that our code measures will mean that services will incur a one-off cost of checking the age of their entire existing user base.¹⁶ To estimate costs illustrative costs, we multiply the number of users by the per-check cost (for example, 100,000 users x 5p = £5,000).
- A3.32 As noted in our general cost assumptions, in practice we expect some services would be able to implement measures PCU B4 – PCU B7 while only conducting age checks on a subset of all users (e.g., those who want access to restricted content). Costs would be lower in those cases.
- A3.33 We also estimate the annual ongoing cost of carrying out age checks for new users. We make illustrative assumptions about the volume of new users, assuming a higher growth rate for smaller services (10%) compared to larger services (1%).
- A3.34 For simplicity, we assume that ongoing age checks on new users will continue, and that: (a) the cost per check remains unchanged over time; (b) all checks for a service cost the same; and (c) the nature of the service does not influence the per-check cost. Table A1.5 sets out a cost estimate for these ongoing checks.
- A3.35 Services may incur other costs including for example software licensing costs, training costs and data storage costs. In most cases we assume these would be included in the ongoing age check costs.
- A3.36 Various testing and evaluation activities are recommended under our highly effective age assurance criteria. Where services use third-party age assurance providers, we expect that those third parties would carry out the bulk of these activities, which may limit further costs incurred by services. However, service providers would still be expected to maintain due oversight and understanding of any third-party testing and evaluation, as it is the

¹⁶ We recognise that in practice this may take place over time as some users may not use the service frequently. We also acknowledge that the requirement to undergo age assurance may result in some user-drop off, which we discuss separately under indirect costs.

service providers in scope of our age assurance measures who are ultimately responsible for ensuring that their approach to age assurance is highly effective. This may therefore require some staff time on an ongoing basis.

- A3.37 Due to the fast-developing age assurance industry and emerging new verification tools the future costs of third-party age methods are uncertain. We think there is a significant likelihood that costs of age assurance will fall over time, as well as the possibility of interoperability of different solutions to increase in the future.

Costs of developing an age assurance method in-house

- A3.38 For illustrative purposes, we have also considered what an age estimation method could cost to develop and run. We assume that the initial phase of work phase may take at least six months, which includes the design, development, testing and deployment of age assurance software. Development time and costs are likely to vary by the approach taken. The estimates we present below are intended to provide an illustrative example of the broad magnitude of costs associated with developing a single in-house age assurance method.

- A3.39 The main costs are likely to be:

- a) One-off labour costs relating to the upfront expense of developing, testing, and deploying the software. This would include ensuring that the age assurance process met the four criteria set out in our guidance: technical accuracy (evaluating methods against appropriate metrics), robustness (evaluating methods in real-world conditions), reliability (producing reproducible results), and fairness (testing and training the method on diverse datasets).
- b) Ongoing staff costs of monitoring, supporting, and maintaining of the age assurance model. This would include meeting recommendations related to reliability, including monitoring key performance indicators and rectifying issues related to unexpected or unreliable predictions.

- A3.40 Our high-level indicative analysis in the context of a large business (which we consider the more likely scenario¹⁷), suggests that the upfront costs of staff involved in the relating to development, testing and deployment of an in-house solution could be in the region of many hundreds of thousands and potentially up to £1 million.¹⁸ The total staff costs, including other non-technical expertise, e.g. legal, may exceed this amount. In addition to these costs, a provider may incur substantial one-off costs relating to acquiring relevant datasets for developing its age assurance method and one-off software/hardware costs relating to additional computational resources to develop and train its age assurance method, which may include cloud infrastructure and data security.¹⁹ A large service may be able to use existing infrastructure and resources for the purpose of a new age assurance

¹⁷ For example, Google has appeared in a registry of providers approved by the Age Check Certification Scheme (ACCS), the UK's program for age verification systems. <https://www.biometricupdate.com/202312/google-receives-certificate-for-facial-age-estimation-in-the-uk> [accessed 7 February 2024].

¹⁸ We assume that the upfront costs are based on staff input on a full-time equivalent (FTE) basis for around six months from c.16 software engineers, while for the ongoing labour costs we assume require c.14 FTEs annually. Costs may increase if the age assurance method involves a particularly high level of expertise, e.g., machine learning. This may be an overestimate given that we expect services could use more junior staff for some model monitoring, maintenance, and support functions.

¹⁹ A service developing an age assurance method is likely to require a cloud security solution that runs all the time and scans information regularly. Securing the data and systems is needed from the development phase but the service will continue to incur this as the systems and data need to be secured on an ongoing basis.

process, there is still an opportunity cost to this because these resources are not available for other uses.

- A3.41 There would also be ongoing staff costs relating to monitoring, evaluation and maintenance, and there could be additional ongoing data costs if the method requires significant improvements and/or changes in the future. We estimate that these ongoing staff costs could reach £1 million annually or potentially more, depending on a service's approach. Our estimates are based on the same salary assumptions for upfront and ongoing costs. In practice, it is possible that some ongoing activities could be conducted by more junior staff on lower salaries, such that ongoing costs could be lower than suggested here.²⁰
- A3.42 As with our examples on third-party methods, these cost estimates are only intended to be illustrative and depend on the different assumptions we have made. The analysis above relates to the development of a single method. Where a service develops multiple methods for use as part of its age assurance process, the total costs are likely to be significantly higher.
- A3.43 Any services seeking to develop age assurance methods in-house are likely to be relatively large, due to the substantial upfront costs relating to software development and testing. This could be more cost effective if a service anticipates a high volume of age checks over time and lower ongoing engineering costs compared to the alternative of using a third-party age assurance provider. Large services may also already have the necessary employees to develop age assurance methods, including those with advanced skills who may be required.
- A3.44 To the extent that smaller services have the relevant capabilities to pursue an in-house approach, it is possible that they may be able to do so more cheaply than suggested by our indicative cost estimates (e.g. due to having simpler organisational processes and lower overheads in relation to the relevant activities).
- A3.45 The service may also incur some one-off staff training costs after age assurance is deployed to users, but these are likely to be relatively small in comparison to the one-off and ongoing costs relating to developing and deploying age assurance approach in-house and will depend primarily on the number of people that need to be trained and how much training is required.

Costs related to appeals related to incorrect assessments of age

- A3.46 Providers may incur costs in relation to handling complaints about incorrect assessments of age. Providers have a duty to allow such complaints to be made and to take appropriate action.²¹ This is discussed further in section 16.

Indirect costs on services

- A3.47 Our research indicates that some users may be reluctant to prove their age due to not wanting to share personal information with a service or concerns about data privacy.²² This may result in some users leaving a service or reducing their usage due to the introduction of highly effective age assurance. The extent of such impacts is likely to be very context-

²⁰ The ongoing labour costs we assume require 14 FTEs annually.

²¹ See Section 21 of the Online Safety Act 2023.

²² Ofcom, 2022, [Adult Users' Attitudes to Age Verification on Adult Sites](#). p. 10. [accessed 2 May 2024].

dependent and is also particularly uncertain in the longer term, as the implementation and adoption of and attitudes towards age assurance evolve.

- A3.48 These impacts will depend on how highly effective age assurance is implemented – for example, whether it is used to age-gate an entire service, or only parts of a service or specific pieces of content. We discuss such impacts in the context of specific measures in section 13.

A4. Legal framework: Duties of providers and Ofcom in relation to the protection of children

This annex sets out the duties relating to the protection of children, as they apply to providers of user-to-user services; providers of search services; and to Ofcom, and which are relevant to this statement.

This annex does not cover other duties set out in the Online Safety Act 2023 (the Act),²³ except where relevant to the protection of children. We have not referred to aspects of the legal and regulatory framework which relate to illegal content, which were covered in our statement entitled December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement).²⁴ We have also not referred to aspects of the legal framework which relate to Phase 3 of our implementation roadmap, such as transparency, user empowerment and other duties on categorised services.

Provider duties in relation to children's access assessments (user-to-user and search)

- A4.1 The Act places providers of regulated user-to-user services and providers of regulated search services under a duty to conduct a suitable and sufficient children's access assessment and to keep a written record of the same, in an easily understandable form.²⁵
- A4.2 A children's access assessment first involves determining whether it is possible for children in the UK to access all or part of the service.^{26 27} The Act provides that a service can only conclude that it is *not* possible for children in the UK to access the service²⁸ if age verification or age estimation is used on the service with the result that children are ordinarily prevented from accessing the service.²⁹
- A4.3 If a provider determines that it is possible for children in the UK to access all or part of the service, the provider must go on to consider whether the child user condition is met in relation to all or the relevant part of that service.³⁰ That will be the case where:

²³ [Online Safety Act 2023](#).

²⁴ Ofcom, 2024. [Statement: Protecting people from illegal harms online](#). See Annex 2 [accessed 26 March 2025].

²⁵ Section 36 of the Act.

²⁶ Section 35(1)(a) and (5)(a) of the Act.

²⁷ Services do not need to assess whether parts of the service which are not, or are not included in, the user-to-user part of the service or a search engine can be accessed by children in the UK. See section 35(5)(b) of the Act.

²⁸ Or the relevant part of the service, as applicable.

²⁹ Section 35(2) of the Act.

³⁰ Section 35(1)(b) of the Act.

- a) There are a significant number of children in the UK who are users of the service or of the relevant part of it, or
 - b) The service, or the relevant part of it, is of a kind likely to attract a significant number of users who are children in the UK.³¹
- A4.4 In relation to limb (a), the Act provides that whether or not the test is met should be assessed using evidence about actual users (and not who the intended users are).³² If the number of users that are children in the UK is significant in proportion to the total number of UK users of the service (or the relevant part of it), then the number of children in the UK who are users is significant.³³
- A4.5 Providers who provide more than one user-to-user or search service must carry out a separate children’s access assessment for each service.³⁴
- A4.6 Part 1 of Schedule 3 to the Act specifies the deadline by which providers must complete their first children’s access assessment. Providers of services in operation immediately before the publication of our Children’s Access Assessments Guidance³⁵ (see paragraph 2.22 of the guidance) are required to complete the first children’s access assessment relating to the service within three months of the date on which that guidance is published (i.e., by 16 April 2025). Providers of services that start up or otherwise become Part 3 services after the publication of our Children’s Access Assessments Guidance must complete their first children’s access assessment within three months of becoming a Part 3 service (see paragraph 2.23 and 2.24 of the guidance).³⁶
- A4.7 If, having conducted a children’s access assessment, a provider determines that a service (or the relevant part of it) is *not* likely to be accessed by children, then it must carry out a further children’s access assessment no more than one year later.³⁷ Such a provider is also required to carry out a further assessment:
- a) Before making any significant change to any aspect of the service’s design or operation to which such an assessment is relevant;
 - b) In response to evidence about reduced effectiveness of age verification or age estimation that is used on the service in order to achieve the result that children are not normally able to access the service or part of it;³⁸ or
 - c) In response to evidence about a significant increase in the number of children using the service.³⁹
- A4.8 Ofcom is required to issue guidance for user-to-user and search services to assist with completing the children’s access assessment.⁴⁰ We first published the Children’s Access

³¹ Section 35(3) of the Act.

³² Section 35(4)(b) of the Act.

³³ Section 35(4)(a) of the Act.

³⁴ Section 36(5) of the Act.

³⁵ [Children’s access assessments](#)

³⁶ Different provisions apply to providers of video-sharing platform (VSP) services currently regulated by Part 4B of the Communications Act 2003 as set out in Part 3 of Schedule 3. However, in practice all VSPs are subject to the same deadlines as other Part 3 services.

³⁷ Section 36(3) of the Act.

³⁸ Section 35(2) of the Act.

³⁹ Section 36(4) of the Act.

⁴⁰ Section 52(3)(b) of the Act.

Assessment Guidance on 16 January 2025 and have republished it with this statement with minor updates.

When services will be likely to be accessed by children

- A4.9 Section 37 of the Act sets out when a service will be treated as likely to be accessed by children for the purposes of the Act.
- a) First, this will be the case where a children's access assessment carried out by the provider of the service concludes that it is possible for children in the UK to access all or part of the service and the child user condition is met in relation to the service or the part of the service that it is possible for children to access (see paragraphs A4.2-A4.5).⁴¹ In that case, the service will be treated as likely to be accessed by children from the date on which the children's access assessment is completed.⁴²
 - b) Second, this will be the case where the provider of the service fails to carry out the first children's access assessment by the deadline specified in Schedule 3 to the Act.⁴³ In that case, the service will be treated as likely to be accessed by children from the date by which the assessment should have been completed until the first children's access assessment has been completed.^{44 45}
 - c) Third, the Act provides that in specific circumstances Ofcom can take action which will result in a service being treated as likely to be accessed by children for the purposes of the Act. This will be the case where, following an investigation into the failure to complete a children's access assessment in accordance with the relevant requirements,⁴⁶ we determine that it is possible for children in the UK to access the service (or the relevant part of it) and the child user condition is met in relation to the service (or the relevant part of it)^{47 48} and, as such mandate that the children's safety duties must be complied with by the provider. In that case, the service will be treated as likely to be accessed by children from the date specified by Ofcom.⁴⁹ Ofcom has the power to specify the circumstances in which the service will cease to be treated as likely to be accessed by children.^{50 51}

⁴¹ Section 37(2) of the Act.

⁴² Section 37(3) of the Act.

⁴³ Section 37(4) of the Act.

⁴⁴ Section 37(5) of the Act.

⁴⁵ If the conclusion of that assessment is that it is possible for children in the UK to access all or part of the service and the child user condition is met, then the service will continue to be treated as likely to be accessed by children by virtue of section 37(2) of the Act.

⁴⁶ Such a failure may arise either in circumstances in which no children's access assessment has been completed at all or in circumstances in which an assessment has been completed but the relevant requirements have not been complied with, for example, because the assessment that has been completed is not suitable and sufficient.

⁴⁷ Sections 135(4) and (5) of the Act give Ofcom the power to make such a determination.

⁴⁸ See paragraphs A4.2-A4.4 for further detail on when it is 'possible for children in the UK to access the service' and the 'child user condition'.

⁴⁹ The date will be specified in a confirmation decision given to the provider of the service under sections 132 and 135 of the Act.

⁵⁰ Section 135(5)(b) of the Act.

⁵¹ The circumstances will be specified in a confirmation decision given to the provider of the service under sections 132 and 135 of the Act.

Duties of providers of user-to-user services likely to be accessed by children

- A4.10 Providers of user-to-user services are given specific duties under the Act in relation to the protection of children. These include the ‘children’s risk assessment duties’⁵² and the ‘safety duties protecting children’.⁵³
- A4.11 Providers of user-to-user services are also subject to ‘additional duties’ which are relevant, among other things, to the protection of children. These additional duties are as follows:
- a) “Duties about content reporting and complaints procedures, which include –
 - i) “duties about content reporting”,⁵⁴ and
 - ii) “duties about complaints procedures”;⁵⁵ and
 - b) So-called ‘cross-cutting duties’, which include –
 - i) “duties about freedom of expression and privacy”,⁵⁶ and
 - ii) “record-keeping and review duties”.⁵⁷
- A4.12 These are set out in more detail below. Section 7 of the Act states that all providers of regulated user-to-user services must comply with these duties (and the other duties set out under section 7(2)).

Connection with the UK

- A4.13 These duties only apply to:
- a) The design, operation and use of the service in the UK, and
 - b) In the case of a duty that is expressed to apply in relation to users of a service, the design, operation and use of the service as it affects UK users of the service.⁵⁸

Combined services

- A4.14 Where the user-to-user service is a combined service (i.e., providing both a regulated user-to-user and regulated search service), these duties will not apply to:
- a) The search content of the service,
 - b) Any other content that, following a search request, may be encountered as a result of subsequent interactions with internet services, or
 - c) Anything relating to the design, operation or use of the search engine.⁵⁹
- A4.15 However, the duties that apply to regulated search services in relation to the protection of children (see paragraphs A4.41-A4.64) will still apply to those aspects of a combined service.⁶⁰

⁵² Section 11 of the Act.

⁵³ Section 12 of the Act.

⁵⁴ Section 20 of the Act.

⁵⁵ Section 21 of the Act.

⁵⁶ Section 22 of the Act.

⁵⁷ Section 23 of the Act.

⁵⁸ Section 8(3) of the Act.

⁵⁹ Section 8(2) of the Act.

⁶⁰ Section 7(6) of the Act.

Safety duties for services likely to be accessed by children

Protection of children risk assessment duties

- A4.16 Providers of regulated user-to-user services that are likely to be accessed by children have a duty to carry out a suitable and sufficient children's risk assessment⁶¹ at the specific times set out in Schedule 3 to the Act.⁶²
- A4.17 A children's risk assessment means an assessment of the following matters, taking into account the risk profiles that relate to the services of that kind:⁶³
- a) The user base, including the number of users who are children in different age groups;
 - b) The level of risk of children who are users of the service encountering the following by means of the service –
 - i) each kind of primary priority content (PPC) that is harmful to children⁶⁴ (with each kind separately assessed),
 - ii) each kind of priority content (PC) that is harmful to children⁶⁵ (with each kind separately assessed), and
 - iii) non-designated content (NDC) that is harmful to children,⁶⁶ giving separate consideration to children in different age groups, and taking into account (in particular) algorithms used by the service and how easily, quickly and widely content may be disseminated by means of the service;
 - c) The level of risk of harm to children presented by different kinds of content that is harmful to children, giving separate consideration to children in different age groups;
 - d) The level of risk of harm to children presented by content that is harmful to children which particularly affects individuals with a certain characteristic or members of a certain group;
 - e) The extent to which the design of the service, in particular its functionalities, affects the level of risk of harm that might be suffered by children, identifying and assessing those functionalities that present higher levels of risk, including functionalities –

⁶¹ Section 11(2) of the Act.

⁶² The deadline for completing the first risk assessment depends on the day on which a provider of user-to-user services starts its operations. In particular:

- i. User-to-user services that are already in operation at the outset of this regime must complete their first children's risk assessment within a period of three months from the day on which Ofcom's [Children's Risk Assessment Guidance](#) is published (i.e., by 24 July 2025);
- ii. New user-to-user services that start operations after the Children's Risk Assessment Guidance is published must complete their first children's risk assessment within a period of three months from the day on which they begin their new services; and
- iii. Existing services that become user-to-user services (having previously provided a different type of service) after the Children's Risk Assessment Guidance is published must complete their first children's risk assessment within a period of three months from the day on which their services become a user-to-user service. See Schedule 3 to the Act.

⁶³ Section 11(6) of the Act.

⁶⁴ See section 61 of the Act for the definition of 'primary priority content that is harmful to children'.

⁶⁵ See section 62 of the Act for the definition of 'priority content that is harmful to children'.

⁶⁶ See section 60(2)(c) and (4) of the Act for the definition of 'non-designated content that is harmful to children'.

enabling adults to search for other users of the service (including children), or
enabling adults to contact other users (including children) by means of the service;

- f) The different ways in which the service is used, including functionalities or other features of the service that affect how much children use the service (e.g., a feature that enables content to play automatically), and the impact of such use on the level of risk of harm that might be suffered by children;
- g) The nature, and severity, of the harm that might be suffered by children from the matters identified in accordance with paragraphs (b) to (f), giving separate consideration to children in different age groups;
- h) How the design and operation of the service (including the business model, governance, use of proactive technology, measures to promote users' media literacy and safe use of the service, and other systems and processes) may reduce or increase the risks identified.

A4.18 The provider of a user-to-user service that is likely to be accessed by children must take appropriate steps to keep a children's risk assessment up to date, including when Ofcom makes a significant change to a relevant risk profile (see paragraph A4.70).⁶⁷

A4.19 The provider of a user-to-user service that is likely to be accessed by children is under an obligation to carry out a further suitable and sufficient children's risk assessment, before making any significant changes to any aspect of a service's design or operation. This further children's risk assessment must relate to the impact of that proposed change.⁶⁸

A4.20 Where a children's risk assessment of a service identifies the presence of NDC that is harmful to children, the provider of the user-to-user service is under duty to notify Ofcom of –

- a) The kinds of such content identified, and
- b) The incidence of those kinds of content on the service.⁶⁹

Safety duties relating to the protection of children

A4.21 Providers of regulated user-to-user services likely to be accessed by children have specific safety duties in relation to children's online safety as set out under section 12 of the Act. These duties extend to such parts of a service as it is possible for children to access.^{70 71} The duties are as follows:

- a) A duty, in relation to a service, to take or use proportionate measures relating to the design or operation of the service to effectively –
 - i) mitigate and manage the risks of harm to children in different age groups, as identified in the most recent children's risk assessment of the service (see paragraph A4.16 and section 11(6)(g) of the Act), and

⁶⁷ Section 11(3) of the Act.

⁶⁸ Section 11(4) of the Act.

⁶⁹ Section 11(5) of the Act.

⁷⁰ A provider is only entitled to conclude that it is not possible for children to access a service, or a part of it, if age verification or age estimation is used on the service with the result that children are not normally able to access the service or that part of it: see section 13(6) of the Act.

⁷¹ Section 13(5) of the Act.

- ii) mitigate the impact of harm to children in different age groups presented by content that is harmful to children present on the service.⁷²
- b) A duty to operate a service using proportionate systems and processes designed to –
 - i) prevent children of any age from encountering, by means of the service, PPC that is harmful to children;⁷³
 - ii) protect children in age groups judged to be at risk of harm from other content that is harmful to children⁷⁴ (or from a particular kind of such content), as assessed by the provider of a service in the most recent children’s risk assessment of the service,⁷⁵ from encountering it by means of the service.⁷⁶
- c) The duty in paragraph i) above requires a provider to use age verification or age estimation (or both) that is of such a kind, and used in such a way, that it is highly effective at correctly determining whether or not a particular user is a child, to prevent children of any age from encountering PPC that is harmful to children which the provider identifies on the service, except where –
 - i) a term of service indicates (in whatever words) that the presence of that kind of PPC that is harmful to children is prohibited on the service, and
 - ii) that policy applies in relation to all users of the service.⁷⁷
- d) A duty to include provisions in the terms of service specifying –
 - i) how children of any age are to be prevented from encountering PPC that is harmful to children (with each kind of PPC separately covered);
 - ii) how children in age groups judged to be at risk of harm from PC that is harmful to children (or from a particular kind of such content), as assessed by the provider of a service in the most recent children’s risk assessment of the service,⁷⁸ are to be protected from encountering it, where they are not prevented from doing so (with each kind of PC separately covered); and
 - iii) how children in age groups judged to be at risk of harm from NDC that is harmful to children (or from a particular kind of such content), as assessed by the provider of a service in the most recent children’s risk assessment of the service,⁷⁹ are to be protected from encountering it, where they are not prevented from doing so.⁸⁰
- e) A duty to apply the provisions of the terms of service referred to in paragraph (d) above consistently.⁸¹
- f) If a provider takes or uses a measure designed to prevent access to the whole of the service or a part of the service by children under a certain age, a duty to –

⁷² Section 12(2) of the Act.

⁷³ With the harm arising by virtue of the nature of the content rather than the fact of its dissemination: see section 13(4) of the Act.

⁷⁴ With the harm arising by virtue of the nature of the content rather than the fact of its dissemination: see section 13(4) of the Act. This includes PC that is harmful to children as well as NDC that is harmful to children.

⁷⁵ Section 13(3) of the Act.

⁷⁶ Section 12(3) of the Act.

⁷⁷ Section 12(4)-(6) of the Act.

⁷⁸ Section 13(3) of the Act.

⁷⁹ Section 13(3) of the Act.

⁸⁰ Section 12(9) of the Act.

⁸¹ Section 12(10) of the Act.

- i) include provisions in the terms of service specifying details about the operation of the measure, and
 - ii) apply those provisions consistently.⁸²
 - g) A duty to include provisions in the terms of service giving information about any proactive technology used by a service for the purpose of compliance with a duty set out in paragraph a) or b) above⁸³ (including the kind of technology, when it is used, and how it works).⁸⁴
 - h) A duty to ensure that the provisions of the terms of service referred to in paragraphs d), e) and f) above⁸⁵ are clear and accessible.⁸⁶
- A4.22 So far as the above duties relate to NDC that is harmful to children, the relevant duty is to be taken to extend only to addressing risks of harm from the kinds of such content that have been identified in the most recent children's risk assessment (if any have been identified).⁸⁷
- A4.23 The duties set out in paragraphs A4.21a) and A4.21b)⁸⁸ apply across all areas of a service, including the way it is designed, operated and used as well as content present on the service, and (among other things) require the provider of a service to take or use measures in the following areas, if it is proportionate to do so:
- a) Regulatory compliance and risk management arrangements,
 - b) Design of functionalities, algorithms and other features,
 - c) Policies on terms of use,
 - d) Policies on user access to the service or to particular content present on the service, including blocking users from accessing the service or particular content,
 - e) Content moderation, including taking down content,
 - f) Functionalities allowing for control over content that is encountered, especially by children,
 - g) User support measures, and
 - h) Staff policies and practices.⁸⁹
- A4.24 Age verification or age estimation to identify who is or is not a child user or which age group a child user is in are examples of measures which (if not required by section 12(4) of the Act: see paragraph A4.21c) may be taken or used (among others) for the purpose of compliance with a duty set out in paragraph A4.21a) or A4.21b).⁹⁰
- A4.25 Providers of Category 1 services likely to be accessed by children are also subject to a duty to summarise in the terms of service the findings of the most recent children's risk assessment of a service (including as to levels of risk and as to nature, and severity, of potential harm to children).⁹¹

⁸² Section 12(11) of the Act.

⁸³ Those paragraphs refer to the provisions in section 12(2) and (3) of the Act.

⁸⁴ Section 12(12) of the Act.

⁸⁵ Those paragraphs refer to the provisions in section 12(9), (11) and (12) of the Act.

⁸⁶ Section 12(13) of the Act.

⁸⁷ Section 13(2) of the Act.

⁸⁸ Those paragraphs refer to the provisions in section 12(2) and (3) of the Act.

⁸⁹ Section 12(8) of the Act.

⁹⁰ Those paragraphs refer to the provisions in section 12(2) and (3) of the Act.

⁹¹ Section 12(14) of the Act.

- A4.26 In determining what is ‘proportionate’ for the purposes of the safety duties set out above, the following factors, in particular, are relevant:
- a) All the findings of the most recent children’s risk assessment (including as to levels of risk and as to nature, and severity, of potential harm to children), and
 - b) The size and capacity of the provider of the service.⁹²

Providers’ judgements about whether content is harmful to children

- A4.27 Section 192 of the Act sets out the approach to be taken by providers to judgements about the status of content including where:
- a) A system or process operated or used by a service provider for the purpose of compliance with relevant requirements (including the duties and requirements under the Act), or
 - b) A risk assessment required to be carried out by Part 3, involves a judgement by a provider about whether content is content of a particular kind.⁹³
- A4.28 Such judgements are to be made on the basis of all relevant information that is reasonably available to a provider, where the following factors, in particular, are relevant:
- a) The size and capacity of the provider; and
 - b) Whether a judgement is made by human moderators, by means of automated systems or processes or by means of automated systems or processes together with human moderators.⁹⁴
- A4.29 In considering a provider’s compliance with section 192 requirements, Ofcom may take into account whether providers’ judgements follow the approaches set out in this section (including judgements made by means of automated systems or processes, alone or together with human moderators).⁹⁵

Duties about content reporting and complaints procedures

- A4.30 The duties about content reporting and complaints procedures for providers of user-to-user services are contained in sections 20 and 21 of the Act.

Duties about content reporting

- A4.31 All providers of regulated user-to-user services are required to use systems and processes in the operation of their services which allow users and ‘affected persons’ to easily report certain types of content, depending on the kind of service. For instance, such systems and processes must be put in place to enable users and affected persons to report “content that is harmful to children, present on a part of a service that it is possible for children to access”⁹⁶ on all user-to-user services likely to be accessed by children.⁹⁷

⁹² Section 13(1) of the Act.

⁹³ Section 192(1) of the Act.

⁹⁴ Section 192(2) and (3) of the Act.

⁹⁵ Section 192(8) of the Act.

⁹⁶ Section 20(6) of the Act states that: “a provider is only entitled to conclude that it is not possible for children to access a service, or a part of it, if age verification or age estimation is used on the service with the result that children are not normally able to access the service or that part of it.”

⁹⁷ Section 20(2) and (4) of the Act.

- A4.32 For the purposes of the duties about content reporting and complaints procedures, an ‘affected person’ means a person, other than a user of the service in question, who is in the UK and who is:
- a) The subject of the content,
 - b) A member of a class or group of people with a certain characteristic targeted by the content,
 - c) A parent of, or other adult with responsibility for, a child who is a user of the service or is the subject of the content, or
 - d) An adult providing assistance in using the service to another adult who requires such assistance, where that other adult is a user of the service or is the subject of the content.⁹⁸
- A4.33 In applying the content reporting duty, the cross-cutting duties will also be relevant (see paragraph A4.36).

Duties about complaints procedures

- A4.34 There are two main duties in respect of complaints procedures which apply in relation to all regulated user-to-user services. These are:
- a) A duty to operate a complaints procedure, in relation to a service, that –
 - i) allows for relevant kinds of complaint to be made (as set out below),
 - ii) provides for appropriate action to be taken by the provider of the service in response to complaints of a relevant kind, and
 - iii) is easy to access, easy to use (including by children) and transparent.⁹⁹
 - b) A duty to include provisions in the terms of service which are easily accessible (including to children) specifying the policies and processes that govern the handling and resolution of complaints of a relevant kind.¹⁰⁰
- A4.35 For services that are likely to be accessed by children¹⁰¹ the following will be a relevant complaint:
- a) Complaints by users and affected persons about content, present on a part of a service that it is possible for children to access, which they consider to be content that is harmful to children;
 - b) Complaints by users and affected persons if they consider that the provider is not complying with the children’s safety duties (see paragraphs A4.21-A4.26);
 - c) Complaints by a user who has generated, uploaded or shared content on a service if that content is taken down, or access to it is restricted, on the basis that it is content that is harmful to children;
 - d) Complaints by a user of a service if the provider has given a warning to the user, suspended or banned the user from using the service, or in any other way restricted the user’s ability to use the service, as a result of content generated, uploaded or

⁹⁸ Section 20(5) of the Act.

⁹⁹ Section 21(2) of the Act.

¹⁰⁰ Section 21(3) of the Act.

¹⁰¹ These categories apply in addition to those types of relevant complaint which apply to all regulated user-to-user services as set out in section 21(4) of the Act. These are covered by the [Illegal Content Codes of Practice for user-to-user services](#) [accessed 26 March 2025]. See Ofcom’s Statement: Protecting people from illegal harms online, [Annex 2](#) (Legal Framework), Part B, paragraph A2.26 for more information. Category 1 services are also required to provide for additional types of relevant complaint, as set out in section 21(6) of the Act.

- shared by the user which the provider considers to be content that is harmful to children; and
- e) Complaints by a user who is unable to access content because measures used to comply with the children's safety duties have resulted in an incorrect assessment of the user's age.¹⁰²

Cross-cutting duties

A4.36 The Act also creates so-called 'cross-cutting duties', which apply to regulated user-to-user services in relation to the performance of *other* duties under the Act as set out in section 22 of the Act (duties about freedom of expression and privacy) and section 23 of the Act (record-keeping and review duties). For instance, the freedom of expression and privacy duties are concerned with how 'safety measures and policies' are introduced in relation to a regulated user-to-user service, while the record-keeping and review duties require the keeping of written records about, and reviewing, how duties relating to the protection of children have been met.

Duties about freedom of expression and privacy

- A4.37 All regulated user-to-user services will have the following duties when deciding on, and implementing, 'safety measures and policies':¹⁰³
- a) A duty to have particular regard to the importance of protecting users' right to freedom of expression within the law;¹⁰⁴ and
 - b) A duty to have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a user-to-user service (including, but not limited to, any such provision or rule concerning the processing of personal data).^{105 106}

Record-keeping and review duties

- A4.38 All regulated user-to-user services likely to be accessed by children will have the following duties:
- a) A duty to make and keep a written record, in an easily understandable form, of every children's risk assessment under section 11 (see paragraphs A4.16 -A4.20).^{107 108}
 - b) A duty to make and keep a written record of any measures taken or in use to comply with a relevant duty which –

¹⁰² Section 21(5) of the Act.

¹⁰³ 'Safety measures and policies' refer to any measures or policies designed to secure compliance with the safety duties relating to the protection of children (section 12 of the Act, paragraphs A4.21-A4.26), and the duties about content reporting (section 20, paragraphs A4.31-A4.33) and complaints procedures (section 21 of the Act, paragraphs A4.34-A4.35), as well as other duties in relation to illegal content (section 10 of the Act), and user empowerment (section 15 of the Act). See section 22(8) of the Act.

¹⁰⁴ Section 22(2) of the Act.

¹⁰⁵ Section 22(3) of the Act.

¹⁰⁶ Additional duties relating to carrying out impact assessments and publishing publicly available statements on impacts of users' rights to freedom of expression and privacy apply to Category 1 services, as set out in section 22(4)-(7) of the Act. These will be covered at a later stage of Ofcom's work.

¹⁰⁷ And every risk assessment under section 9 of the Act (illegal content risk assessment duties). Category 1 services are also required, as soon as reasonably practicable after making or revising a record of a risk assessment, to supply Ofcom with a copy of the record in full – see section 23(9) of the Act.

¹⁰⁸ Section 23(2) of the Act.

- i) are described in a code of practice and recommended for the purpose of compliance with the duty in question, and
 - ii) apply in relation to the provider and the service in question. Such measures are referred to as “applicable measures in a code of practice”.¹⁰⁹
 - c) If alternative measures (see paragraph A4.39) have been taken or are in use to comply with a relevant duty, a duty to make and keep a written record containing the following information –
 - i) the applicable measures in a code of practice that have not been taken or are not in use,
 - ii) the alternative measures that have been taken or are in use,
 - iii) how those alternative measures amount to compliance with the duty in question, and
 - iv) how the provider has had regard to the importance of protecting the right of users to freedom of expression within the law, and protecting the privacy of users in taking or using alternative measures.¹¹⁰
 - d) A duty to review compliance with the relevant duties in relation to a service –
 - i) regularly, and
 - ii) as soon as reasonably practicable after making any significant change to any aspect of the design or operation of the service.¹¹¹
- A4.39 ‘Alternative measures’ means measures other than measures which are (in relation to the provider and the service in question) applicable measures in a code of practice.¹¹² If alternative measures have been taken or are in use to comply with any of the safety duties relating to the protection of children set out in section 12(2) or (3) of the Act (see paragraphs A4.21a and A4.21b)),¹¹³ these records must also indicate whether such measures have been taken or are in use in every area listed at paragraph A4.23¹¹⁴ in relation to which there are applicable measures in a code of practice (see paragraphs A4.74-A4.100).¹¹⁵
- A4.40 As required under section 52(3)(a) of the Act, we published guidance on record keeping and review as part of our December 2024 Statement.¹¹⁶ This guidance has been updated and published alongside this statement to reflect the duties relevant to services likely to be accessed by children: see Volume 3, paragraph 8.207.

¹⁰⁹ Section 23(3) of the Act.

¹¹⁰ Section 23(4) of the Act. See also section 49(5) of the Act.

¹¹¹ Section 23(6) of the Act.

¹¹² Section 23(11) of the Act.

¹¹³ Or with the safety duties about illegal content (section 10(2) or 10(3) of the Act).

¹¹⁴ These are the areas listed in section 12(8) of the Act.

¹¹⁵ Similarly, if alternative measures have been taken or are in use to comply with the safety duties about illegal content in section 10(2) or 10(3) of the Act, these records must also indicate whether such measures have been taken or are in use in every area listed in section 10(4) of the Act in relation to which there are applicable measures in a Code.

¹¹⁶ See Ofcom, 2024. [Record-Keeping and Review Guidance](#) [accessed 26 March 2025]. Subsequent references to this source throughout.

Duties of providers of search services likely to be accessed by children

- A4.41 Providers of regulated search services are also given specific duties under the Act in relation to the protection of children. These include ‘children’s risk assessment duties’,¹¹⁷ and ‘safety duties protecting children’.¹¹⁸
- A4.42 Providers of regulated search services are also subject to additional duties which are relevant to the protection of children, but also apply to other types of content and in respect of other regulatory requirements as set out under the Act. These are:
- a) “Duties about content reporting and complaints procedures”, which include –
 - i) the “duty about content reporting”,¹¹⁹ and
 - ii) “duties about complaints procedures”;¹²⁰ and
 - b) The ‘cross-cutting duties’, which include:
 - i) “duties about freedom of expression and privacy”;¹²¹ and
 - ii) “record-keeping and review duties”.¹²²
- A4.43 These are set out in more detail below. Section 24 of the Act states that all providers of regulated search services must comply with these duties (and the other duties set out under section 24(2)).

Connection with the UK

- A4.44 These duties only apply to:
- a) The search content of the service;
 - b) The design, operation and use of the search engine in the UK; and
 - c) In the case of a duty that is expressed to apply in relation to users of a service, the design, operation and use of the search engine as it affects UK users of the service.¹²³

Combined services

- A4.45 Where a service is a combined service (i.e., providing both a regulated user-to-user and regulated search service), the duties applying to user-to-user services likely to be accessed by children will apply save for in relation to:
- a) The search content of the service;
 - b) Any other content that, following a search request, may be encountered as a result of subsequent interactions with internet services; or
 - c) Anything relating to the design, operation or use of the search engine.¹²⁴

¹¹⁷ Section 28 of the Act.

¹¹⁸ Section 29 of the Act.

¹¹⁹ Section 31 of the Act.

¹²⁰ Section 32 of the Act.

¹²¹ Section 33 of the Act.

¹²² Section 34 of the Act.

¹²³ Section 25(1) of the Act.

¹²⁴ Section 25(2) of the Act.

Safety duties for services likely to be accessed by children

Protection of children risk assessment duties

- A4.46 Providers of regulated search services that are likely to be accessed by children have a duty to carry out a suitable and sufficient children's risk assessment¹²⁵ at the specific times set out in Schedule 3 to the Act.¹²⁶
- A4.47 A children's risk assessment means an assessment of the following matters, taking into account the risk profiles that relate to the services of that kind:¹²⁷
- a) The level of risk of children who are users of the service encountering search content of the following kinds –
 - i) each kind of PPC that is harmful to children¹²⁸ (with each kind separately assessed),
 - ii) each kind of PC that is harmful to children¹²⁹ (with each kind separately assessed), and
 - iii) NDC that is harmful to children,¹³⁰ giving separate consideration to children in different age groups, and taking into account (in particular) risks presented by algorithms used by the service and the way that the service indexes, organises and presents search results;
 - b) The level of risk of children who are users of the service encountering search content that is harmful to children which particularly affects individuals with a certain characteristic or members of a certain group;
 - c) The extent to which the design of the service, in particular its functionalities, affects the level of risk of harm that might be suffered by children, identifying and assessing those functionalities that present higher levels of risk, including a functionality that makes suggestions relating to users' search requests (predictive search functionality);
 - d) The different ways in which the service is used, including functionalities or other features of the service that affect how much children use the service, and the impact of such use on the level of risk of harm that might be suffered by children;

¹²⁵ Section 28(2) of the Act.

¹²⁶ The deadline for completing the first risk assessment depends on the day on which a search service's provider starts its operations. In particular:

- i. Search services that are already in operation at the outset of this regime must complete their first children's risk assessment within a period of three months from the day on which our Children's Risk Assessment Guidance is published (i.e., by 24 July 2025);
- ii. New search services that start operations after the Children's Risk Assessment Guidance is published must complete their first children's risk assessment within a period of three months from the day on which they begin their new services; and
- iii. Existing services that become search services (having previously provided a different type of service) after the Children's Risk Assessment Guidance is published must complete their first children's risk assessment within a period of three months from the day on which their services become a search service. See Schedule 3 to the Act.

¹²⁷ Section 28(5) of the Act.

¹²⁸ See section 61 of the Act for the definition of 'primary priority content that is harmful to children'.

¹²⁹ See section 62 of the Act for the definition of 'priority content that is harmful to children'.

¹³⁰ See section 60(2)(c) and (4) of the Act for the definition of 'non-designated content that is harmful to children'.

- e) The nature, and severity, of the harm that might be suffered by children from the matters identified in accordance with paragraphs (a) to (d), giving separate consideration to children in different age groups; and
- f) How the design and operation of the service (including the business model, governance, use of proactive technology, measures to promote users' media literacy and safe use of the service, and other systems and processes) may reduce or increase the risks identified.

A4.48 The provider of a search service that is likely to be accessed by children must take appropriate steps to keep a children's risk assessment up to date, including when Ofcom makes a significant change to a relevant risk profile (see paragraph A4.70).¹³¹

A4.49 The provider of a search service that is likely to be accessed by children is under an obligation to carry out a further suitable and sufficient children's risk assessment, before making any significant changes to any aspect of a service's design or operation. This further children's risk assessment must relate to the impact of that proposed change.¹³²

Safety duties relating to the protection of children

A4.50 Providers of regulated search services likely to be accessed by children have specific safety duties in relation to children's online safety as set out under section 29 of the Act. These duties extend to such parts of a service as it is possible for children to access.¹³³ The duties are as follows:

- a) A duty, in relation to a service, to take or use proportionate measures relating to the design or operation of the service to effectively –
 - i) mitigate and manage the risks of harm to children in different age groups, as identified in the most recent children's risk assessment of the service (section 28(5)(e) of the Act), and
 - ii) mitigate the impact of harm to children in different age groups presented by content that is harmful to children present on the service.¹³⁴
- b) A duty to operate a service using proportionate systems and processes designed to –
 - i) minimise the risk of children of any age encountering search content that is PPC that is harmful to children;¹³⁵ and
 - ii) minimise the risk of children in age groups judged to be at risk of harm from other content that is harmful to children¹³⁶ (or from a particular kind of such content), as assessed by the provider of a service in the most recent children's risk assessment of the service,¹³⁷ encountering search content of that kind.¹³⁸

¹³¹ Section 28(3) of the Act.

¹³² Section 28(4) of the Act.

¹³³ Section 30(5) of the Act. A provider is only entitled to conclude that it is not possible for children to access a service, or a part of it, if age verification or age estimation is used on the service with the result that children are not normally able to access the service or that part of it: see section 30(6) of the Act.

¹³⁴ Section 29(2) of the Act.

¹³⁵ With the harm arising by virtue of the nature of the content rather than the fact of its dissemination: see section 30(4) of the Act.

¹³⁶ With the harm arising by virtue of the nature of the content rather than the fact of its dissemination: see section 30(4) of the Act.

¹³⁷ Section 30(3) of the Act.

¹³⁸ Section 29(3) of the Act.

- c) A duty to include provisions in a publicly available statement specifying how children are to be protected from search content of the following kinds –
 - i) PPC that is harmful to children (with each kind of PPC separately covered),
 - ii) PC that is harmful to children (with each kind of PC separately covered), and
 - iii) NDC that is harmful to children.¹³⁹
 - d) A duty to –
 - i) ensure that the provisions of the publicly available statement referred to in paragraph A4.50(c) are applied consistently;¹⁴⁰
 - ii) include provisions in a publicly available statement giving information about any proactive technology (see paragraphs A4.92-A4.96) used by a service for the purpose of compliance with a duty set out in paragraph a) or b) (including the kind of technology, when it is used and how it works);¹⁴¹ and
 - iii) ensure that the provisions of the publicly available statement are clear and accessible.¹⁴²
- A4.51 So far as the above duties relate to NDC that is harmful to children, the relevant duty is to be taken to extend only to addressing risks of harm from the kinds of such content that have been identified in the most recent children’s risk assessment (if any have been identified).¹⁴³
- A4.52 The duties set out in paragraphs A4.50a) and A4.50b) (section 29(2) and (3) of the Act) apply across all areas of a service, including the way the search engine is designed, operated and used as well as search content of the service, and (among other things) require the provider of a service to take or use measures in the following areas, if it is proportionate to do so:
- a) Regulatory compliance and risk management arrangements,
 - b) Design of functionalities, algorithms and other features relating to the search engine,
 - c) Functionalities allowing for control over content that is encountered in search results, especially by children,
 - d) Content prioritisation,
 - e) User support measures, and
 - f) Staff policies and practices.¹⁴⁴
- A4.53 Providers of Category 2A services likely to be accessed by children are additionally subject to a duty to summarise in a publicly available statement the findings of the most recent children’s risk assessment of a service (including as to levels of risk and as to nature, and severity, of potential harm to children).¹⁴⁵
- A4.54 In determining what is ‘proportionate’ for the purposes of the safety duties for search services likely to be accessed by children, the following factors, in particular, are relevant:
- a) All the findings of the most recent children’s risk assessment (including as to levels of risk and as to nature, and severity, of potential harm to children), and

¹³⁹ Section 29(5) of the Act.

¹⁴⁰ Section 29(6) of the Act.

¹⁴¹ Section 29(7) of the Act.

¹⁴² Section 29(8) of the Act.

¹⁴³ Section 30(2) of the Act.

¹⁴⁴ Section 29(4) of the Act.

¹⁴⁵ Section 29(9) of the Act.

- b) The size and capacity of the provider of a service.¹⁴⁶

Duties about content reporting and complaints procedures

Duty about content reporting

- A4.55 All providers of regulated search services are required to operate a service using systems and processes that allow users and ‘affected persons’ to easily report certain types of search content, depending on the type of service.¹⁴⁷
- A4.56 For services that are likely to be accessed by children, the duty applies in respect of content that is harmful to children.¹⁴⁸
- A4.57 For the purposes of the duties about content reporting and complaints procedures, an ‘affected person’ has the same definition as for user-to-user services (see paragraph A4.32).

Duties about complaints procedures

- A4.58 There are two main duties in respect of complaints procedures which apply in relation to all regulated search services. These are as follows:
- a) A duty to operate a complaints procedure in relation to a service that –
 - i) allows for relevant kinds of complaint to be made (as set out below),
 - ii) provides for appropriate action to be taken by the provider of the service in response to complaints of a relevant kind, and
 - iii) is easy to access, easy to use (including by children) and transparent.¹⁴⁹
 - b) A duty to make the policies and processes that govern the handling and resolution of complaints of a relevant kind publicly available and easily accessible (including to children).¹⁵⁰
- A4.59 For services that are likely to be accessed by children¹⁵¹ the following will be a relevant complaint:
- a) Complaints by users and affected persons about search content which they consider to be content that is harmful to children;
 - b) Complaints by users and affected persons if they consider that the provider is not complying with the children’s safety duties (see paragraphs A4.50-A4.54);
 - c) Complaints by an interested person if the provider of a search service takes or uses measures in order to comply with the children’s safety duties that result in content relating to that interested person no longer appearing in search results or being given a lower priority in search results; and

¹⁴⁶ Section 30(1) of the Act.

¹⁴⁷ Section 31(2) of the Act.

¹⁴⁸ Section 31(4) of the Act.

¹⁴⁹ Section 32(2)(a)-(c) of the Act.

¹⁵⁰ Section 32(3) of the Act.

¹⁵¹ These categories apply in addition to those types of relevant complaint which apply to all regulated search services as set out in section 32(4) of the Act. These are covered by the Illegal Content Codes of Practice for user-to-user services. See our December 2024 Statement, [Annex 2](#) (Legal Framework), Part B, paragraph A2.51 for more information.

- d) Complaints by a user who is unable to access content because measures used to comply with the children’s safety duties described in paragraphs A4.50a) and A4.50b)¹⁵² have resulted in an incorrect assessment of the user’s age.¹⁵³
- A4.60 For the purposes of the duties about complaints procedures for regulated search services, an ‘interested person’ means a person that is responsible for a website or database capable of being searched by the search engine, provided that:
- a) In the case of an individual, the individual is in the UK;
 - b) In the case of an entity, the entity is incorporated or formed under the law of any part of the UK.¹⁵⁴

Cross-cutting duties

- A4.61 The Act also creates ‘cross-cutting’ duties which apply to regulated search services in relation to the performance of other duties under the Act, as set out in section 33 of the Act (duties about freedom of expression and privacy) and section 34 of the Act (record-keeping and review duties). For instance, the duties about freedom of expression and privacy are concerned with how ‘safety measures and policies’ are introduced in relation to a regulated search service, while the record-keeping and review duties require the keeping of written records about, and reviewing, how duties relating to the protection of children have been met.

Duties about freedom of expression and privacy

- A4.62 All regulated search services will have the following duties when deciding on, and implementing, ‘safety measures and policies’:¹⁵⁵
- a) A duty to have particular regard to the importance of protecting the rights of users and interested persons to freedom of expression within the law;¹⁵⁶ and
 - b) A duty to have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a search service (including, but not limited to, any such provision or rule concerning the processing of personal data).¹⁵⁷

Record-keeping and review duties

- A4.63 All regulated search services will have the following duties:

¹⁵² These are the duties in section 29(2) and (3) of the Act.

¹⁵³ Section 32(5)(a)-(d) of the Act.

¹⁵⁴ Sections 32(6) and 227(7) of the Act.

¹⁵⁵ ‘Safety measures and policies’ refer to any measures or policies designed to secure compliance with the safety duties relating to the protection of children (section 29, paragraphs A4.50-A4.54), and the duties about content reporting (section 31, paragraphs A4.55-A4.57) and complaints procedures (section 32, paragraphs A4.58-A4.60), as well as other duties in relation to illegal content (section 27).

¹⁵⁶ Section 33(2) of the Act.

¹⁵⁷ Section 33(3) of the Act.

- a) A duty to make and keep a written record, in an easily understandable form, of every children’s risk assessment made under section 28.^{158 159}
- b) A duty to make and keep a written record of any measures taken or in use to comply with a relevant duty which –
 - i) are described in a code of practice and recommended for the purpose of compliance with the duty in question, and
 - ii) apply in relation to the provider and the service in question. In this section such measures are referred to as ‘applicable measures in a code of practice’.¹⁶⁰
- c) If alternative measures have been taken or are in use to comply with a relevant duty, a duty to make and keep a written record containing the following information –
 - i) the applicable measures in a code of practice that have not been taken or are not in use,
 - ii) the alternative measures that have been taken or are in use,
 - iii) how those alternative measures amount to compliance with the duty in question, and
 - iv) how the provider has had regard to the importance of protecting the right of users and interested persons to freedom of expression within the law, and protecting the privacy of users in taking or using alternative measures (i.e., under section 49(5)).¹⁶¹
- d) If alternative measures have been taken or are in use to comply with the safety duties about the protection of children (specifically section 29(2) or (3)), this record must also indicate whether such measures have been taken or are in use in every area listed at section 29(4) (or section 27(4) of the Act as the case may be) in relation to which there are applicable measures in a code of practice.¹⁶²
- e) A duty to review compliance with the relevant duties in relation to a service: regularly, and as soon as reasonably practicable after making any significant change to any aspect of the design or operation of the service.¹⁶³

A4.64 As required under section 52(3)(a) of the Act, we published guidance on record keeping and review as part of our December 2024 Statement.¹⁶⁴ This guidance has been updated and published alongside this statement to reflect the duties relevant to services likely to be accessed by children: see Volume 3, paragraph 8.207.

Ofcom’s duties in relation to the protection of children

A4.65 The Act gives specific duties to Ofcom in relation to the protection of children. These are set out below.

¹⁵⁸ Section 34(2) of the Act.

¹⁵⁹ And every risk assessment under section 26 (illegal content risk assessments). In addition, Category 2A services are required, as soon as reasonably practicable after making or revising a record of a risk assessment, to supply Ofcom with a copy of the record in full – see section 34(9) of the Act.

¹⁶⁰ Section 34(3) of the Act.

¹⁶¹ Section 34(4)(a)-(d) of the Act.

¹⁶² Section 34(5) of the Act.

¹⁶³ Section 34(6)(a) and (b) of the Act.

¹⁶⁴ See Ofcom, 2024. Record-Keeping and Review Guidance.

Ofcom sector risk assessment

- A4.66 Ofcom is under a duty to carry out a risk assessment to identify and assess the risks of harm to children in the UK, in different age groups, presented by content that is harmful to children.^{165 166}
- A4.67 Ofcom's risk assessment must, among other things, identify the characteristics of user-to-user and search services (which include functionalities, user base, business model and governance, and other systems and processes) that are relevant to the risks of harm and assess the impact of these characteristics on the risks of harm.¹⁶⁷

Children's Register of Risks and Children's Risk Profiles

- A4.68 Ofcom must prepare and publish a register of risks that reflects the findings of its sector risk assessment (Children's Register).¹⁶⁸ The Children's Register must be prepared as soon as reasonably practicable after completion of the risk assessment.¹⁶⁹
- A4.69 Further to the Children's Register, after completing its risk assessments, Ofcom must prepare and publish risk profiles for user-to-user services and search services that relate to each risk of harm, as applicable (the Children's Risk Profiles, which are incorporated in the Children's Risk Assessment Guidance). In preparing the Children's Risk Profiles, Ofcom can group user-to-user services and search services as appropriate and having regard to (i) the characteristics of the services and (ii) the risk levels and other matters identified in the risk assessment.¹⁷⁰
- A4.70 Ofcom must review and revise the risk assessments and the Children's Risk Profiles from time to time to keep them up to date.¹⁷¹

Risk assessment guidance for services

- A4.71 Ofcom must prepare and publish guidance to help user-to-user services and search services comply with their duties to prepare children's risk assessments under sections 11 and 28 respectively (the Children's Risk Assessment Guidance).¹⁷²
- A4.72 Ofcom must prepare the Children's Risk Assessment Guidance as soon as reasonably practicable after having published the risk profiles relating to the risks of harm to children.¹⁷³
- A4.73 Ofcom must revise and publish updated Children's Risk Assessment Guidance when it carries out a new risk assessment and/or revises the risk profiles.¹⁷⁴

¹⁶⁵ Section 98(1)(c) of the Act.

¹⁶⁶ Ofcom has discretion in relation to whether to combine the risk assessments with the risk assessments relating to illegal content it is required to carry out under section 98(1)(a) and (b) of the Act. Ofcom may assess regulated user-to-user services and regulated search services separately or together. Section 98(3) of the Act.

¹⁶⁷ Section 98(2) and (11) of the Act.

¹⁶⁸ [\[link to children's register\]](#)

¹⁶⁹ Section 98(4) of the Act.

¹⁷⁰ Section 98(5)-(7) of the Act.

¹⁷¹ Section 98(8) of the Act.

¹⁷² Section 99(3) and (6) of the Act.

¹⁷³ Section 99(3) of the Act.

¹⁷⁴ Section 99(5) of the Act.

Protection of Children Codes of Practice for user-to-user and search

Ofcom's duty to prepare and issue Protection of Children Codes of Practice in relation to the protection of children

- A4.74 Ofcom must issue Protection of Children Codes of Practice (Codes) for regulated user-to-user and search services containing measures recommended for the purposes of compliance with certain duties including:
- a) The protection of children safety duties in sections 12 and 29;¹⁷⁵
 - b) The content reporting duties in sections 20 and 31;¹⁷⁶ and
 - c) The complaints procedure duties in sections 21 and 32.¹⁷⁷
- A4.75 Schedule 4 to the Act sets out general principles and online safety objectives which the Codes must follow, as well as what content must be included. These are set out below.

General principles

- A4.76 In preparing a draft code, Ofcom must consider the appropriateness of provisions of the code to different kinds and sizes of user-to-user and search services, and to providers of differing sizes and capacities (paragraph 1 of Schedule 4). It must also have regard to the following principles:
- a) Providers of user-to-user and search services must be able to understand which provisions of the code of practice apply in relation to a particular service they provide;
 - b) The measures described in the code of practice must be sufficiently clear, and at a sufficiently detailed level, that providers understand what those measures entail in practice;
 - c) The measures described in the code of practice must be proportionate and technically feasible: measures that are proportionate or technically feasible for providers of a certain size or capacity, or for services of a certain kind or size, may not be proportionate or technically feasible for providers of a different size or capacity or for services of a different kind or size; and
 - d) The measures described in the code of practice that apply in relation to user-to-user and search service providers of various kinds and sizes must be proportionate to Ofcom's assessment of the risk of harm presented by services of that kind or size (see paragraph A4.66).¹⁷⁸

Online safety objectives

- A4.77 Ofcom must ensure that measures described in the Codes are compatible with the pursuit of the online safety objectives.¹⁷⁹
- A4.78 For user-to-user services, the online safety objectives are:
- a) That a service should be designed and operated in such a way that –

¹⁷⁵ Section 41(3) and (10)(b) of the Act.

¹⁷⁶ Section 41(3) and (10)(f) of the Act.

¹⁷⁷ Section 41(3) and (10)(g) of the Act.

¹⁷⁸ Paragraph 2(a)-(d) of Schedule 4 to the Act.

¹⁷⁹ Paragraph 3 of Schedule 4 to the Act.

- i) the systems and processes for regulatory compliance and risk management are effective and proportionate to the kind and size of service,
 - ii) the systems and processes are appropriate to deal with the number of users of the service and its user base,
 - iii) UK users (including children) are made aware of, and can understand, the terms of service,
 - iv) there are adequate systems and processes to support UK users,
 - v) (in the case of a Category 1 service) users are offered options to increase their control over the content they encounter and the users they interact with,
 - vi) the service provides a higher standard of protection for children than for adults,
 - vii) the different needs of children at different ages are taken into account,
 - viii) there are adequate controls over access to the service by adults, and
 - ix) there are adequate controls over access to, and use of, the service by children, taking into account use of the service by, and impact on, children in different age groups; and
- b) That a service should be designed and operated so as to protect individual UK users from harm, including with regard to –
- algorithms used by the service,
- i) functionalities of the service, and
 - ii) other features relating to the operation of the service.¹⁸⁰

A4.79 For search services, the online safety objectives are:

- a) That a service should be designed and operated in such a way that –
 - i) the systems and processes for regulatory compliance and risk management are effective and proportionate to the kind and size of service,
 - ii) the systems and processes are appropriate to deal with the number of users of the service and its user base,
 - iii) UK users (including children) are made aware of, and can understand, the publicly available statement referred to in relation to the safety duties protecting children in section 29,¹⁸¹
 - iv) there are adequate systems and processes to support UK users,
 - v) the service provides a higher standard of protection for children than for adults, and
 - vi) the different needs of children at different ages are taken into account; and
- b) That a service should be assessed to understand its use by, and impact on, children in different age groups; and
- c) That a search engine should be designed and operated so as to protect individuals in the UK who are users of the service from harm, including with regard to –
 - i) algorithms used by the search engine,
 - ii) functionalities relating to searches (such as a predictive search functionality), and
 - iii) the indexing, organisation and presentation of search results.¹⁸²

¹⁸⁰ Paragraph 4 of Schedule 4 to the Act.

¹⁸¹ This provision also applies to the statement relating to the illegal content safety duties referred to in section 27 of the Act.

¹⁸² Paragraph (5)(a)-(c) of Schedule 4 to the Act.

A4.80 For combined services:

- a) The online safety objectives that apply to user-to-user services (paragraph A4.78) do not apply in relation to the search engine;
- b) The online safety objectives that apply to search services apply in relation to the search engine (and, accordingly, in this context, references to a search service are to be read as references to the search engine); and
- c) The reference to a publicly available statement includes a reference to provisions of the terms of service which relate to the search engine.¹⁸³

A4.81 The Secretary of State may amend these objectives by way of regulations.¹⁸⁴

Content of Codes of Practice

A4.82 The Act also sets out what type of measures must be included in the content of the various Codes, and the principles in light of which such measures should be designed. In particular:

- a) Codes that describe measures recommended for the purpose of compliance with the safety duties for providers of user-to-user services (i.e., in relation to taking proportionate measures relating to the design or operation of the service, or to operate a service using proportionate systems and processes),¹⁸⁵ must include measures in each of the areas of a service listed at paragraph A4.23.^{186 187}
- b) Codes that describe measures recommended for the purpose of compliance with the safety duties for providers of search services (i.e., in relation to taking proportionate measures relating to the design or operation of the service, or to operate a service using proportionate systems and processes)¹⁸⁸ must include measures in each of the areas of a service listed at paragraph A4.52.^{189 190}
- c) The requirements outlined in (a) and (b) above apply to the extent that inclusion of the measures in question is consistent with paragraph 1(a) of Schedule 4¹⁹¹ and the principles outlined in paragraph 2(c) and (d) of Schedule 4.^{192 193}

A4.83 Any measures described in a code of practice which are recommended for the purpose of compliance with any of the relevant duties must be designed in the light of the following principles:

- a) The importance of protecting the right of users and (in the case of search services or combined services) interested persons to freedom of expression within the law, and

¹⁸³ Paragraph 6(a)-(c) of Schedule 4 to the Act.

¹⁸⁴ Paragraph 7 of Schedule 4 to the Act.

¹⁸⁵ These are the measures in section 12(2) and (3) of the Act.

¹⁸⁶ These are the areas listed in section 12(8) of the Act.

¹⁸⁷ Paragraph 9(2) of Schedule 4 to the Act.

¹⁸⁸ These are the measures in section 29(2) and (3) of the Act.

¹⁸⁹ These are the areas listed in section 29(4) of the Act.

¹⁹⁰ Paragraph 9(4) of Schedule 4 to the Act.

¹⁹¹ This requires Ofcom to consider the appropriateness of provisions of the code of practice to different kinds and sizes of Part 3 services and to providers of differing sizes and capacities.

¹⁹² These are that the measures described in the code of practice must be proportionate and technically feasible, and proportionate to Ofcom's assessment of the risk of harm presented by services of that kind or size.

¹⁹³ Paragraph 9(5) of Schedule 4 to the Act.

b) The importance of protecting the privacy of users.¹⁹⁴

A4.84 Where appropriate, such measures must also incorporate safeguards for the protection of the matters mentioned in those principles.

A4.85 Such measures may only relate to the design or operation of the relevant service in the UK, or as it affects UK users of the service.¹⁹⁵

Age assurance

A4.86 In deciding whether to recommend the use of age assurance, or which kinds of age assurance to recommend, in a code of practice as a measure recommended for the purpose of compliance with any of the duties set out in paragraphs A4.21a) or A4.21b)¹⁹⁶ (these apply to user-to-user services) or paragraphs A4.50a) or A4.50b)¹⁹⁷ (these apply to search services) Ofcom must, in addition to the general principles and principles in relation to freedom of expression and privacy set out above,¹⁹⁸ have regard to the following:

- a) The principle that age assurance should be effective at correctly identifying the age or age-range of users;
- b) Relevant standards set out in the latest version of the code of practice under section 123 of the Data Protection Act 2018 (age-appropriate design code);
- c) The need to strike the right balance between –
 - i) the levels of risk and the nature, and severity, of potential harm to children which the age assurance is designed to guard against, and
 - ii) protecting the right of users and (in the case of search services or the search engine of combined services) interested persons to freedom of expression within the law;
- d) The principle that more effective kinds of age assurance should be used to deal with higher levels of risk of harm to children;
- e) The principle that age assurance should be easy to use, including by children of different ages and with different needs;
- f) The principle that age assurance should work effectively for all users regardless of their characteristics or whether they are members of a certain group; and
- g) The principle of interoperability between different kinds of age assurance.¹⁹⁹

A4.87 If a code of practice does recommend age assurance for the purpose of complying with the duties set out paragraphs A4.21a) or A4.21b)²⁰⁰ (these apply to user-to-user services) then it must also describe measures for the purpose of complying with the following duties:

- a) The duties regarding the inclusion of clear information in the terms of service described in paragraphs A4.21c)-f);²⁰¹ and

¹⁹⁴ This refers to protecting the privacy of users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a user-to-user or search service (including any provisions concerning the processing of personal data), paragraph 10(2) and (3) of Schedule 4 to the Act.

¹⁹⁵ Paragraph 11 of Schedule 4 to the Act.

¹⁹⁶ These are the duties in section 12(2) or (3) of the Act.

¹⁹⁷ These are the duties in section 29(2) or (3) of the Act.

¹⁹⁸ Paragraph 12(1) of Schedule 4 to the Act.

¹⁹⁹ Paragraph 12(1) and (2) of Schedule 4 to the Act.

²⁰⁰ These are the duties in section 12(2) or (3) of the Act.

²⁰¹ These are the duties in section 12(9), (11) and (13) of the Act.

- b) The duties regarding complaints about age assurance described in paragraph A4.35.²⁰²
- A4.88 If a code of practice does recommend age assurance for the purpose of complying with the duties set out in paragraphs A4.50a) or A4.50b)²⁰³ (these apply to search services) then it must also describe measures for the purpose of complying with the following duties:
- a) The duties regarding the inclusion of clear information in the publicly available statement described in paragraphs A4.50c) and d);²⁰⁴ and
 - b) The duties regarding complaints about age assurance.²⁰⁵
- A4.89 A provider of a user-to-user service likely to be accessed by children is required to use age verification or age estimation (or both) to prevent children of any age from encountering PPC that is harmful to children which the provider identifies on the service.²⁰⁶ 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.²⁰⁷
- A4.90 Part 5 of the Act imposes specific duties on service providers that display or publish pornographic content on their online services. Further detail is set out below at paragraphs A4.104-A4.106. In decision which kinds and uses of age verification or age estimation for the purposes of compliance with the duty set out in section 12(3)(a) of the Act, Ofcom must have regard to the guidance issued in relation to examples of kinds and uses of age verification and estimation that are, or are not, highly effective at correctly determining whether or not a particular user is a child.²⁰⁸
- A4.91 The Act makes clear that a code of practice may:
- a) Refer to industry or technical standards for age assurance (where they exist); and/or
 - b) Elaborate on the principles mentioned in paragraphs (a) and (c) to (g) of paragraph A4.86 (in relation to age assurance).²⁰⁹

Proactive technology

- A4.92 If Ofcom considers it appropriate to do so, and in accordance with the general principles set out at paragraphs 1 and 2 of Schedule 4 and the principles set out at paragraph 10(2) of Schedule 4, it may include in a code of practice a measure describing the use of a kind of technology.²¹⁰ However, there are constraints on Ofcom's power to include a measure describing the use of 'proactive technology' (a 'proactive technology measure').²¹¹ Section 231 of the Act defines 'proactive technology' as consisting of three types of technology: content identification technology, user profiling technology, and behaviour identification technology (subject to certain exceptions set out in section 231(3) and (7)). These are explained in greater detail below.

²⁰² These are the duties in section 21(2) and (3) of the Act. See in particular section 21(5)(e) (complaints about age assurance).

²⁰³ These are the duties in section 29(2) or (3) of the Act.

²⁰⁴ These are the duties in section 29(5) and (8) of the Act.

²⁰⁵ These are the duties in section 32(2), (3) and (5)(d) of the Act.

²⁰⁶ Section 12(3)(a) and (4) of the Act.

²⁰⁷ Section 12(6) of the Act.

²⁰⁸ Paragraph 12(4) of Schedule 4 to the Act.

²⁰⁹ Paragraph 12(8) of Schedule 4 to the Act.

²¹⁰ Paragraph 13(1) of Schedule 4 to the Act.

²¹¹ Paragraph 13(2) of Schedule 4 to the Act.

- A4.93 **‘Content identification technology’** refers to technology, such as algorithms, keyword matching, image matching or image classification, which analyses content to assess whether it is content of a particular kind (e.g., illegal content). Content identification technology is not regarded as proactive technology if it is used in response to a report from a user or other person about particular content.²¹²
- A4.94 **‘User profiling technology’** means technology which analyses (any or all of) relevant content (as defined in section 231(8)), user data, or metadata relating to relevant content or user data, for the purposes of building a profile of a user to assess characteristics such as age. However, technology which analyses data specifically provided by a user for the purposes of the provider verifying or estimating the user’s age in order to decide whether to allow the user to access a service (or part of a service) or particular content, but which does not analyse any other data or content, is not regarded as user profiling technology.²¹³
- A4.95 **‘Behaviour identification technology’** means technology which analyses (any or all of) relevant content (as defined in section 231(8)), user data, or metadata relating to relevant content or user data, to assess a user’s online behaviour or patterns of online behaviour (e.g., to assess whether a user may be involved in, or be the victim of, illegal activity). However, behaviour identification technology is not regarded as proactive technology if it is used in response to concerns identified by another person or an automated tool about a particular user.²¹⁴
- A4.96 Ofcom has power to include a proactive technology measure in a code of practice for the purpose of compliance with the safety duties in relation to the protection of children described in paragraphs A4.21a) or A4.21b)²¹⁵ (these apply to user-to-user services) or paragraphs A4.50a) or A4.50b)²¹⁶ (these apply to search services).²¹⁷ However, that power is subject to the following constraints:
- a) A proactive technology measure may relate to the use of a kind of technology on or in relation to any Part 3 service or any part of such a service, but if the technology operates (or may operate) by analysing user-generated content or metadata relating to such content, the measure may not recommend the use of technology which operates (or may operate) by analysing user-generated content communicated privately, or metadata relating to such content.²¹⁸
 - b) A proactive technology measure may be included in a code of practice in relation to services of a particular kind or size only if Ofcom is satisfied that the use of the technology by such services would be proportionate to the risk of harm that the measure is designed to safeguard against (taking into account, in particular, Ofcom’s risk profile relating to such services published under section 98).²¹⁹

²¹² Section 231(2) and (3) of the Act.

²¹³ Section 231(4) and (5) of the Act.

²¹⁴ Section 231(6) and (7) of the Act.

²¹⁵ These are the duties in section 12(2) or (3) of the Act.

²¹⁶ These are the duties in section 29(2) or (3) of the Act.

²¹⁷ Paragraph 13(3) of Schedule 4 to the Act. A proactive technology measure may also be recommended for the purpose of compliance with the illegal content safety duties set out in section 10(2) or (3) of the Act (in relation to user-to-user services) or section 27(2) or (3) of the Act (in relation to search services), or for the purpose of compliance with the fraudulent advertising duties set out in section 38(1) or 39(1) of the Act.

²¹⁸ See paragraph 13(4) of Schedule 4 to the Act. For factors which Ofcom must particularly consider when deciding whether content is communicated ‘publicly’ or ‘privately’ by means of a user-to-user service for these purposes: see section 232 of the Act.

²¹⁹ See paragraph 13(5) of Schedule 4 to the Act.

- c) In deciding whether to include a proactive technology measure in a code of practice, Ofcom must have regard to the degree of accuracy, effectiveness and lack of bias achieved by the technology in question. Ofcom may also refer in the code of practice to existing industry or technical standards for the technology (where they exist), or set out principles in the code of practice designed to ensure that the technology or its use is (so far as possible) accurate, effective and free of bias.²²⁰

Relationship between provider duties and Ofcom's Codes of Practice

- A4.97 Providers of a regulated user-to-user or search service who take or use the measures described in a code of practice which are recommended for the purpose of complying with a relevant duty will be treated as having complied with that relevant duty.²²¹ Further, providers who take or use the relevant recommended measures that incorporate safeguards to protect users' rights to freedom of expression within the law, and to protect the privacy of users, respectively, will be treated as having complied with the freedom of expression and privacy duties set out in paragraph A4.37 (for user-to-user services)²²² and paragraph A4.62 (for search services).^{223 224}
- A4.98 Where a provider adopts an alternative measure to those described in a code of practice in order to comply with a relevant duty, it must have particular regard to the importance of protecting the right of users and (in the case of search services) interested persons to freedom of expression within the law, and protecting the privacy of users.²²⁵
- A4.99 When assessing whether a provider of a service that has adopted alternative measures is compliant with a duty to protect children's online safety, Ofcom must consider the extent to which the alternative measures taken or in use by the provider extend across all areas of a service listed in sections 12(8) or 29(4) (if relevant to the duty in question), and, where appropriate, incorporate safeguards for the protection of the right of users and (in the case of search services) interested persons to freedom of expression within the law, and protection of the privacy of users.²²⁶

Effect of the Codes of Practice

- A4.100 Failure to comply with a provision of a code of practice does not in itself make the provider liable to legal proceedings in a court or tribunal,²²⁷ although the code will be admissible in evidence in legal proceedings,²²⁸ and any such court or tribunal must take a provision of the code into account when determining a question arising in any proceedings which is relevant to that provision, and relates to a time when the provision was in force.²²⁹ Similarly, Ofcom must take into account a provision of a code of practice when determining a question arising in connection with the exercise of any relevant function if the question is relevant to that provision, and relates to a time when the provision was in force.²³⁰

²²⁰ See paragraph 13(6) of Schedule 4 to the Act. This requirement does not apply to proactive technology which is a kind of age verification or age estimation technology: see paragraph 13(7) of Schedule 4 to the Act.

²²¹ Section 49(1) of the Act.

²²² These are the duties in section 22(2) and (3) of the Act.

²²³ These are the duties in section 33(2) and (3) of the Act.

²²⁴ Section 49(2)-(3) of the Act.

²²⁵ Section 49(5) of the Act.

²²⁶ Section 49(6) of the Act.

²²⁷ Section 50(1) of the Act.

²²⁸ Section 50(2) of the Act.

²²⁹ Section 50(3) of the Act.

²³⁰ Section 50(4) of the Act.

Children’s Access Assessments Guidance

A4.101 Ofcom is required to issue guidance for user-to-user and search services to assist with determining whether their services are likely to be accessed by children (i.e. completing the children’s access assessment).²³¹ See our Children’s Access Assessments Guidance which we first published on 16 January 2025 and have republished with this statement with minor updates.

Guidance on Content Harmful to Children

A4.102 Ofcom must produce guidance which gives examples of content that Ofcom considers to be (or not to be) PPC and PC that is harmful to children.²³² See our [Guidance on Content Harmful to Children](#), published alongside this statement.

Record-Keeping and Review Guidance

A4.103 Ofcom must produce guidance for providers of regulated user-to-user and search services to assist them in complying with their record-keeping and review duties (sections 23 (user-to-user) and 34 (search)) – paragraphs A4.38-A4.40 (user-to-user), and A4.63-A4.64 (search).²³³ We produced this guidance as part of the December 2024 Statement.²³⁴ We have also updated this guidance to reflect the duties as relevant to services likely to be accessed by children.²³⁵ This guidance has been updated and published alongside this statement to reflect the duties relevant to services likely to be accessed by children: see Volume 3, paragraph 8.207.

Part 5 guidance

A4.104 Duties in Part 5 of the Act (the Part 5 duties) apply where regulated provider pornographic content (as defined in section 79 of the Act) is published or displayed by a provider of an internet service (or on behalf of such a provider) on that internet service. These duties include a requirement for service providers to implement highly effective age assurance to ensure that children are not normally able to encounter regulated provider pornographic content displayed on their service.²³⁶

A4.105 Ofcom must produce guidance for providers of internet services which fall within scope of Part 5 to help them comply with the duties outlined above.²³⁷ To that end, Ofcom must include examples of the kinds and uses of age assurance that are, or are not, highly effective at determining whether or not a user is a child. The guidance must also set out the principles that Ofcom proposes to apply when determining if a service provider has complied with the duties in section 81 of the Act, and examples of circumstances where we are likely to consider that they have not complied with each of those duties.²³⁸ See our

²³¹ Section 52(3)(b) of the Act.

²³² Section 53 of the Act.

²³³ Section 52(3) of the Act.

²³⁴ Ofcom, 2024. Record-Keeping and Review Guidance.

²³⁵ Ofcom, 2025. Record-Keeping and Review.

²³⁶ Section 81(2) and (3) of the Act.

²³⁷ Section 82(1) of the Act.

²³⁸ Section 82(2) of the Act.

Guidance on highly effective age assurance and other Part 5 duties²³⁹ for more information on the Part 5 duties and the services to which they apply.

- A4.106 In addition to the Part 5 guidance, we also issued Guidance on highly effective age assurance, published on 16 January 2025 and republished with this statement with minor updates, to assist providers of regulated user-to-user and search services (Part 3 services) in implementing highly effective age assurance for the purpose of fulfilling their regulatory obligations under the Act.²⁴⁰ We have sought to ensure a consistent approach to highly effective age assurance across the Part 5 guidance and the Part 3 guidance on highly effective age assurance to ensure consistency so that service providers in scope of both Part 5 and Part 3 of the Act are clear on what they need to do to prevent children from encountering the most harmful forms of content.

²³⁹ [Guidance on highly effective age assurance and other Part 5 duties](#)

²⁴⁰ [Guidance on highly effective age assurance](#)

A5. Equality Impact Assessment and Welsh Language Assessment

This annex sets out the legal framework underpinning our equality impact assessment and Welsh language impact assessment duties and our final equality and Welsh language impact assessments for decisions in this protection of children statement. In updating our assessment, we have considered and responded to stakeholder feedback on the equality and Welsh language impact assessment we consulted on in our May 2024 Consultation on Protecting Children from Harms Online (May 2024 Consultation).

Equality legal framework

- A5.1 Section 149 of the Equality Act 2010 (the 2010 Act) imposes a duty on Ofcom, when carrying out its functions, to have due regard to the need to eliminate discrimination, harassment, victimisation and other prohibited conduct related to the following protected characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex and sexual orientation.
- A5.2 The 2010 Act also requires Ofcom to have due regard to the need to advance equality of opportunity and foster good relations between persons who share specified protected characteristics and persons who do not.
- A5.3 Section 75 of the Northern Ireland Act 1998 (the 1998 Act) also imposes a duty on Ofcom, when carrying out its functions relating to Northern Ireland, to have due regard to the need to promote equality of opportunity and have regard to the desirability of promoting good relations across a range of categories outlined in the 1998 Act. Ofcom's Revised Northern Ireland Equality Scheme explains how we comply with our statutory duties under the 1998 Act.²⁴¹
- A5.4 When thinking about equality, we think more broadly than persons that share protected characteristics identified in equalities legislation and think about potential impacts on various groups of persons (see paragraph 4.7 of our impact assessment guidance).²⁴² Equality impact assessments help us to comply with our duties under section 3 of the Communications Act 2003 (the 2003 Act). Section 3(4)(h) requires Ofcom to have regard to the vulnerability of children, whose circumstances put them in need of special protection. Due to overlap with the protected characteristics under the Equality Act 2010 and the Northern Ireland Act 1998, we have had regard as a part of our Equality Impact Assessment to the vulnerability of those whose circumstances appear to put them in need of special protection and the needs of persons with disabilities and of the elderly. In the context of the Codes, we have focused on the vulnerability of children whose circumstances appear to put them in need of special protection, including those with disabilities and the interests of

²⁴¹ Ofcom, 2014. [Revised Northern Ireland Equality Scheme for Ofcom](#).

²⁴² Ofcom, 2023. [Impact assessment guidance](#).

children in different parts of the UK, who are part of different ethnic communities and who live in both rural and urban areas.²⁴³

- A5.5 We have had regard to the different interests of persons (particularly children) without distinction between the people living in different parts of the UK. This reflects the fact that the Codes apply to services in scope of regulations so far as relevant to the design and operation of their service in the UK or the design, operation and use of the service as it affects UK users.²⁴⁴ While we have had regard to the different interests of persons living in rural and urban areas, we do not consider that there is any relevant difference in these interests for the purposes of our decisions in this document.

Equality Impact Assessment

- A5.6 This statement focuses particularly on the risks of harm to children and the benefits and impacts of the Codes on children, in light of their vulnerability. This is a particular focus of the Act and relates to our obligations under section 3(4)(h) of the 2003 Act. As such, when considering relevant protected characteristics, we have had particular regard to children with those relevant protected characteristics, and this has been central to our decisions as set out within the statement. Further to this, we have set out our approach to the consideration of children's rights at Section 2 of Volume 1 in the statement.
- A5.7 In the following paragraphs we set out a summary of our equality impact assessment position at consultation together with a summary of the stakeholder responses to that impact assessment that were received.

Our position at consultation

- A5.8 In our May 2024 Consultation on Protecting Children from Harms Online (May 2024 Consultation), we set out our impact assessments, including our equality impact assessment and Welsh language assessment, at Annex 14.²⁴⁵
- A5.9 We considered that some of our proposals would have a positive impact on certain groups, and particularly children who form part of those groups, and that most of these impacts were likely to come from the draft Protection of Children Codes.²⁴⁶ We also considered that positive impacts would come from our draft Guidance on Content Harmful to Children. At consultation, we did not consider that any of our proposals would have a detrimental impact on those groups.²⁴⁷

Summary of stakeholder responses

- A5.10 We received feedback from the Northern Ireland Commissioner for Children and Young People (NICCY) that we had not indicated that we had undertaken an equalities impact assessment as required by the section 75 statutory duties of the Northern Ireland Act 1998

²⁴³ Section 3(4) of the 2003 Act.

²⁴⁴ Section 8(3) and section 25(1) of the Act for user-to-user and search services respectively.

²⁴⁵ [Annex 14 of our May 2024 Consultation](#) p.61 to 65.

²⁴⁶ In our May 2024 Consultation we referred to these as the draft Children's Safety Codes.

²⁴⁷ May 2024 Consultation, Annex 14.

and identified the impact of these proposals on children and young people, as well as any associated consultation.²⁴⁸

- A5.11 Violence against women and girls (VAWG) Sector Experts suggested that our focus on age-gating certain services and content may mean that other issues are inadequately addressed. They raised that such issues include the importance of good quality information for children and young people particularly in relation to issues surrounding women's rights, gender equality, and issues affecting girls, such as sexual education or discussions on reproductive rights.²⁴⁹ They cited a Glitch response to our November 2023 Consultation that, “[w]e have seen this censorship already in the reproductive justice space and LGBTQ+ rights. These important and diverse perspectives and experiences may be underrepresented or excluded in search results and content moderation decisions, leading to a narrower range of voices and lower quality information available.”²⁵⁰ They said that measures to improve the breadth and depth of good quality content and information are essential alongside measures to protect from harm.
- A5.12 We have separately set out stakeholder feedback and our response as far as relevant to equality issues in relation to particular aspects of the Codes measures in paragraph A5.26 to A5.56.

Our final assessment

- A5.13 As set out in this statement, we have considered stakeholder feedback in response to the consultation. While we have decided to broadly confirm our proposed measures, we have made some amendments in response to further evidence and feedback from stakeholders regarding the measures within the Codes, as well as our own internal analysis. In making the changes, we have considered the impacts of the Codes, including in relation to rights and costs, as set out within the statement for each measure, as well as considering the impact of the Codes on children with relevant protected characteristics and, where applicable, the impact on adults with protected characteristics more generally.
- A5.14 We have concluded in this final equality impact assessment that any negative impact that the Codes may have on people with any specific protected characteristics or other relevant characteristics or vulnerabilities (other than age), or on equality of opportunity or the fostering of good relations, compared to people without these characteristics, are unlikely to be material. Where the Codes may result in some negative impacts – for example, in respect to adults who may experience additional friction in their user experience as a result of the Codes – we consider that such impacts are justified and proportionate in light of the objectives of the relevant duties in the Act and equality legislation.
- A5.15 We acknowledge that our decisions are likely to have a material impact on the online experiences of adults in the UK, who will, for example, have to undertake age assurance processes as a result of our measures, or who may have other protections applied to them even where they may prefer not to have these, as outlined in the relevant sections of the statement. We have explained why we think the impacts on adult users from our decisions are proportionate in our rights impact assessments throughout the statement, given the

²⁴⁸ NICCY response to May 2024 Consultation, p.8.

²⁴⁹ VAWG Sector Experts response to May 2024 Consultation, p.7.

²⁵⁰ VAWG Sector Experts response to May 2024 Consultation, p.7.

importance of securing a higher standard of protection for children from harm in line with the underlying objectives and duties in the Act.

- A5.16 We received feedback from many stakeholders that the Codes should apply differently to different age groups of children. We acknowledge that while some of the measures encourage providers to consider appropriate action for children in different age groups, the Codes seek to establish a strong baseline level of protection for children of all ages and that older children may consider this to exclude them from certain digital spaces by virtue of the protected characteristic of age. Since consultation, we have made some changes further to consideration of stakeholder responses to take account of potential differential impacts on children in different age groups. Our approach seeks to balance protecting children of all ages from harmful content online with ensuring that children older children (specifically, 16 and 17 year olds) are not impaired in their ability to benefit from digital services in a disproportionate way. In particular, we have made clarifications and changes to the Content Moderation (section 14), Search Moderation (section 15) and Recommender Systems (section 17) measures to reflect the principle that providers should put in place the strongest protections where the benefits to children are greatest and support children to have age-differentiated online experiences, in recognition of the rights and evolving capacities of children as they age. However, we are clear that stronger protections for younger children should not leave older children unprotected.
- A5.17 We will assess and consult on the potential impacts of future recommendations on protected characteristics in future iterations of the Codes and guidance. We expect our evidence base and understanding in this regard to develop over time, and to be able to iterate on the Codes to incorporate changes based on such evidence.
- A5.18 As detailed in this annex, examples of groups that might disproportionately experience, and be negatively affected by, content that is harmful to children includes, but is not limited to, girls impacted by suicide, self-harm, eating disorder and pornographic content, as well as abuse and hate content targeted at women and girls; people of races (and ethnicities) which may be subject to targeted hate and abuse; children of increased vulnerability, who may be particularly psychologically impacted by content that is harmful to children including content which encourages, promotes or provides instructions for suicide, self-harm and eating disorders; and boys, who are more likely than girls to participate in dangerous stunts and challenges and to seek out violent content.
- A5.19 As explained in our May 2024 Consultation, we consider that most of the positive impacts of our decisions on certain groups are likely to come from the recommended measures in our Protection of Children Codes of Practice, as set out in paragraph A5.26 to A5.56.

Children’s Register of Risks, Children’s Risk Profiles and Children’s Risk Assessment Guidance

- A5.20 Ofcom is under a duty to carry out a risk assessment to identify and assess the risks of harm to children in the UK, in different age groups, presented by content that is harmful to children.²⁵¹
- A5.21 Ofcom must prepare and publish a register of risks that reflects the findings of its sector-wide risk assessment (the Children’s Register of Risks), and Risk Profiles for user-to-user

²⁵¹ Section 98(1) of the Act.

services and search services that relate to each risk of harm, as applicable (the Children's Risk Profiles).²⁵² Ofcom must also prepare and publish guidance to help user-to-user services and search services comply with their duties to prepare children's risk assessments under sections 11 and 28 respectively (the Children's Risk Assessment Guidance).²⁵³

- A5.22 Our Children's Register of Risks (the Register) includes evidence of the harm from content that is harmful to children experienced by vulnerable users, and particularly users with multiple protected characteristics. Examples of groups that might disproportionately experience and be negatively affected by content that is harmful to children includes, but is not limited to, girls impacted by suicide, self-harm, eating disorder and pornographic content, as well as abuse and hate content targeted at women and girls; people of races (and ethnicities) which may be subject to targeted hate and abuse; children of increased vulnerability, who may be particularly psychologically impacted by content that is harmful to children including content which encourages, promotes or provides instructions for suicide, self-harm and eating disorders; and boys, who may be more likely than girls to participate in dangerous stunts and challenges and to seek out violent content. Based on evidence in the Register, we have included information in the Children's Risk Profiles to ensure that providers understand and take account of risks to people with protected characteristics. In our Children's Risk Assessment Guidance, we explain that services in scope should consider the demographics of their UK user base, including groups with protected characteristics.

Guidance on Content Harmful to Children

- A5.23 Our Guidance on Content Harmful to Children aims to assist providers when making judgements on content by providing examples of, or kinds of content that we consider to be, or not to be, primary priority content (PPC) and priority content (PC) that is harmful to children. We consider that the examples included within the guidance will have positive equality impacts for people with protected characteristics.
- A5.24 We provide examples of content which we consider to be or not to be content which is abusive or incites hatred and targets any one of a number of characteristics listed in the Act (listed characteristics), which are race, religion, sex, sexual orientation, disability and gender reassignment (abuse and hate content).²⁵⁴ While it is important to acknowledge that the definitions set out in the Act and what they mean in that context differ from some of the protected characteristics set out within the 2010 Act, there is a degree of overlap and similarity. For example, under the Act, 'disability' means any physical or mental impairment whereas under the 2010 Act, a person has a disability if they have a physical or mental impairment, and the impairment has a substantial and long-term adverse effect on the person's ability to carry out normal day-to-day activities. Therefore, 'disability' under the Act is broader than the definition in the 2010 Act.²⁵⁵
- A5.25 We consider that our approach and examples of such content are appropriately balanced such that the listed characteristics under the Act are equally considered when assessing such content. This is likely to result in positive impacts where providers are able to identify and use appropriate measures (as set out in paragraph A5.26 to A5.56) against such

²⁵² Section 98(5) of the Act.

²⁵³ Section 99(3) of the Act.

²⁵⁴ Sections 62(2) and 62(3) of the Act.

²⁵⁵ Section 16(7) of the Act.

content where this might disproportionately impact those with the relevant protected characteristics under the 2010 Act to the extent that they may be impacted by abuse and hate content as defined under the Act.

Protection of Children Codes

Governance and accountability

- A5.26 The Governance and Accountability measures support robust governance processes as an effective way of ensuring good risk management practices within a service. We consider that these measures may benefit those who may be more impacted than others by content that is harmful to children.
- A5.27 For example, providers of in scope of measure PCU A5/PCS A5 are required to track: (a) new kinds of PPC or PC and (b) unusual increases in (i) particular kinds of content that is harmful to children (this includes non-designated content (NDC) that has been identified as a risk in their most recent risk assessment) and (ii) content that is harmful to children proxy.²⁵⁶ We consider that measures such as this (in particular by including content that is harmful to children proxy which is a new addition since our consultation) should lead to more risk mitigation and ultimately increased protection for children with characteristics that mean they are likely to be targeted by, or particularly at risk of, such content.

Terms of service and publicly available statements

- A5.28 The measures relating to terms of service and publicly available statements promote comprehensibility of language, which may benefit people with protected characteristics that could affect their level of literacy.
- A5.29 Benefits could accrue to younger users, people who may not have English as a first language (which can be associated with race) and people with relevant disabilities.
- A5.30 For example, providers creating clear and accessible written information in line with Measure PCU G3/PCS G3 should design these with accessibility in mind, so that they can be used by those dependent on accessibility technologies, which would also benefit (both children and adults) with disabilities.

Age assurance

- A5.31 Our Age Assurance measures aim to help ensure children are protected from harmful content by ensuring that providers in scope of these measures have a highly effective age assurance process that can be used to target relevant protections at children. We have reflected concerns about accessibility in these measures in two ways: firstly, in the criterion for highly effective age assurance relating to fairness, which is reflected in the definition of highly effective age assurance in the Codes; and secondly, in the principle around accessibility which is set out in PCU B1 of the Codes.
- A5.32 In relation to the criterion of fairness, our definition of highly effective age assurance in the Codes, and the Part 3 Guidance on highly effective age assurance,²⁵⁷ states that service providers should ensure that any elements of the age assurance process which rely on

²⁵⁶ This refers to PPC, PC and NDC identified in the provider's terms of service or publicly available statement (as relevant) as subject to moderation action and has also been included to reflect the amendments made to the Content Moderation and Search Moderation measures (see sections 14 and 15 of this statement).

²⁵⁷ [Part 3 Guidance on highly effective age assurance](#).

artificial intelligence or machine learning have been tested and trained on data sets which reflect the diversity in the target population.

- A5.33 Measure PCU B1 sets out the principles that apply to user-to-user services likely to be accessed by children that implement an age assurance process under the Codes. These principles include the recommendation that providers should have regard to ensuring age assurance is easy to use, including by children of different ages and with different needs, and that age assurance should work effectively for all users regardless of their characteristics or whether they are members of a certain group. We have expanded on what the accessibility principle means in relation to age assurance in our Part 3 Guidance on highly effective age assurance. Building these principles into the Codes and the Part 3 Guidance on highly effective age assurance helps protect the interests of children with relevant protected characteristics who may otherwise be affected by the exclusionary impact of age assurance technologies.
- A5.34 Taken together, we conclude these aspects of our regulation will minimise any unintended exclusionary effects of age assurance on children or adults with relevant protected characteristics.

Content moderation for user-to-user services and search services

- A5.35 The Content Moderation measures for user-to-user and search services aim to reduce the amount of content harmful to children that children might encounter by recommending that providers have in place content moderation systems and processes designed to review, assess and take appropriate moderation action when a provider becomes aware of the existence of this type of content.
- A5.36 We received stakeholder feedback on the user-to-user content moderation measures and their potential impacts for equality. Open Rights Group were concerned that the proposed content moderation measures were likely to have negative impacts on people from minority language, culture and sexual minorities, as they rely on content curation which, in their view, generally disfavours minority content.²⁵⁸ We also received a response from the British, Irish Law, Education and Technology Association (BILETA) regarding the measure for resourcing content moderation teams appropriately, that content moderation staff should not only be able to speak relevant languages fluently but also be familiar with “prejudicial terminology”.²⁵⁹
- A5.37 We also considered feedback from Big Brother Watch on the potentially negative impacts of content moderation for minority groups, depending on how “harmful” content is interpreted by providers. They referred to their own report that stated content that engages “harmful stereotypes” can be inappropriately censored. They provided the examples of women on Twitter (now, X) having their accounts temporarily limited, suspended or banned and tweets removed for posting that men are more likely to commit violent crime than women – despite this assertion being supported by data from the Office for National Statistics.²⁶⁰ Big Brother Watch also argued that providers taking down content deemed “harmful” does not tackle the root cause which is the behaviour of individuals, only temporarily stifling it, but that individuals can open further accounts to

²⁵⁸ Open Rights Group response to May 2024 Consultation, p.17.

²⁵⁹ BILETA response to November 2023 Consultation, p.6.

²⁶⁰ Big Brother Watch response to May 2024 Consultation, p.6.

continue harmful behaviours, limiting the protective capacity of content moderation action by providers.

- A5.38 We consider that these measures will enhance protection for children with protected characteristics, including race (which encompasses nationality, ethnic and national origins and may include language insofar as language discrimination may constitute indirect race discrimination), sexual orientation, sex and gender re-assignment due to the disproportionate impact of harmful content on children from groups with these relevant protected characteristics. As outlined in our draft Guidance: A safer life online for women and girls, improvements to content moderation can embed understanding of online gender-based harms into their systems and processes, which are likely to improve outcomes for girls.²⁶¹ Additionally, the content moderation resourcing measure (PCU C6/PCS C6) recommends that providers should have regard to the language needs of their UK user base when resourcing their content moderation function, which may in turn have positive effects for children of different nationalities or ethnic backgrounds. This means that there should not be a disproportionate risk of content from minority groups being removed without reason.
- A5.39 The measures relating to internal content policies (PCU C3/PCS C3) and providing appropriate training and materials to individuals working in moderation (PCU C7/PCS C7) should improve the ability of moderators to identify harmful content effectively and accurately (including types of content harmful to children that might particularly affect groups with protected characteristics) and ensure consistency of decision-making. These measures will address cases where a lack of contextual understanding beyond language creates a gap in the understanding of individuals working in moderation in relation to a particular harm on a service. Overall, these measures will heighten the scope of protection of children by better equipping moderation teams and helping to reduce harmful content, including content types that may disproportionately impact children from groups with relevant protected characteristics, including race.
- A5.40 Further, the recommendation that providers have processes to update their internal content policies in response to evidence of emerging risks (PCU C3/PCS C3) should particularly benefit groups with protected characteristics, who may be targeted by, or particularly at risk of, content harmful to children that may experience periods of increased prevalence and therefore risk. This is similarly promoted by the measures recommending that providers have regard to severity of potential harm to child users (including whether the content is suspected to be PPC, PC or NDC) when setting a policy for prioritisation for review of content (PCU C5/PCS C5).
- A5.41 We acknowledge that the Content Moderation measures for both search services and user-to-user services may result in some negative impacts for adult users. In our rights assessments of the measures set out in Section 14 (Content Moderation) and Section 15 (Search Moderation), we acknowledge that there may be impacts on some users (especially adult users). For example, where access to an adult user's content is restricted for children following a determination that it is content harmful to children, or where service providers choose (in the exercise of their own rights to freedom of expression) to restrict all users' access to content that is harmful to children (or equivalent) under their terms or statements. Additionally, Search Moderation Measure PCS C1 recommends that appropriate moderation action be taken for all users, including adults (except those where

²⁶¹ [Annex A Draft Guidance: a safer life online for women and girls](#), p.57.

the provider has reasonable grounds to determine are adults), and there is also a risk of adult users being incorrectly determined to be children for the purpose of applying the filtering of PPC recommended by Measure PCS C2.

- A5.42 More generally, one potential negative impact may be over-moderation, where providers choose to define the kinds of content that will be subject to moderation more widely than defined in the Act or choose to apply access controls on a user-to-user service to a greater extent than necessary in response to the measures. We have set out in our impact assessments why we consider the measures to be proportionate to the benefits to children, including those with protected characteristics, and the objectives of the Act.

User reporting and complaints

- A5.43 The Reporting and Complaints measures (Section 16) aim to increase accessibility of these procedures by users, including children and affected persons (as defined by the Act).²⁶² Easier reporting processes are likely to benefit groups that may be disproportionately affected by content harmful to children, including abuse and hate content that targets individuals with certain listed characteristics.
- A5.44 Easier reporting and transparent complaint systems may also result in positive impacts for those with protected characteristics which affect their level of literacy. The measures recommend that service providers have regard to the particular needs of a service's UK user base (including children), which includes the needs of people with relevant disabilities.
- A5.45 We received feedback from stakeholders about clarifying and strengthening the measures to increase accessibility and effectiveness of reporting and complaints processes, which we discuss these in Section 16, paragraphs 16.170 to 16.195. We have made minor changes to measures PCU D2/PCS D2 to recommend that providers have regard to industry standards and good practice when designing these systems, together with any other information the service provider may hold about its UK user base. Our aim is that accessibility for child users is increased, by making the process for submitting a complaint as straightforward as possible. This is likely to have positive impacts on child users, with protected characteristics.

Recommender systems on user-to-user services

- A5.46 The Recommender Systems measures aim to exclude content indicated to potentially be PPC from children's recommender feeds (Measure PCU E1), exclude or give a low degree of prominence to content indicated to potentially be PC and NDC in children's recommender feeds (Measure PCU E2), and provide children with a means to give negative feedback on pieces of content that appear in their recommender feeds (Measure PCU E3). These measures aim to reduce the risk of children encountering content that is harmful to them via recommender systems, which includes abuse and hate content that does not meet the criminal threshold and that may target people with certain listed characteristics as noted above. This also includes suicide, self-harm and eating disorder content, where the risk of harm from encountering such content may be exacerbated by existing vulnerabilities. By reducing the likelihood of encountering this content, these measures are likely to have positive impacts for the safety and wellbeing of children that form part of groups that may be disproportionately affected by such content (particularly children with relevant protected characteristics).

²⁶² Section 20(5) of the Act.

- A5.47 Since consultation, we have changed the application of Measure PCU E2 and PCU E3 in relation to NDC. PCU E2 now also applies where service providers identify a medium or high risk of one or more types of NDC in their latest children's risk assessment, and PCU E3 now extends to providers of large services who identify a medium or high risk of least two kinds of PPC, PC and/or any kind of NDC in their latest children's risk assessment. We consider that these changes will lead to greater protections for children, including those who may particularly impacted by particular types of harmful content.

User support

- A5.48 The User Support measures aim to reduce the risk of children encountering content harmful to children and to minimise the impact of harm to children of such content. In particular, we have set out measures relating to the provision of supportive information when children restrict their interaction with other users or content (PCU F2), the signposting of children to support at key points of the user journey (PCU F3-5), and the provision of age-appropriate user support materials (PCU F1/PCS F4). We consider that such measures may benefit children with protected characteristics who may be more impacted than others by content that is harmful to children by providing them with appropriate support.
- A5.49 Since consultation, we have also expanded the application of measures for blocking and muting (PCU J1) and for disabling comments (PCU J2) to apply to additional categories so that each now applies to suicide, self-harm and eating disorder content. Though we have narrowed the segmentation in terms of service size to which these measures apply (by adding application to providers with 700,000 users that have a medium risk of relevant harms), we consider that adding the additional types of harm will add protection for vulnerable children who may be in need of greater protection or have relevant protected characteristics, who may be disproportionately impacted by such content, or girls and those suffering from mental health conditions, who are at increased risk from such types of content.
- A5.50 In relation to the measure on age-appropriate user support materials (PCU F1 and PCS F4 for user-to-user services and search services respectively), when implementing this measure, we explain that these materials should be easy to find on the service (for user-to-user services) and searchable via internal search functionalities (for search services). We also recommend that they be clear, comprehensible and easy for children to understand, which particularly benefit children with relevant protected characteristics that affect their level of literacy. We also recommend the inclusion of at least one of the following kinds of elements: visual elements, audio-visual elements and interactive elements. As well as aiding in the comprehensibility of these materials for children, this could especially benefit children with relevant disabilities or those who may not have English as a first language.

Search features, functionalities and user support

- A5.51 These measures aim to minimise the risk of children encountering content that is harmful to children on or via search services and to mitigate the risk of harm children face from such content when it is encountered.
- A5.52 Measure PCS F1 recommends that providers offer users a means to easily report predictive search suggestions. The recommendation within this measure that reporting functions be prominently displayed is likely to benefit those with protected characteristics by increasing the visibility and accessibility of this reporting function. The measure also recommends that where a provider considers that reported predictive search suggestions present a risk

of users encountering PPC and PC, steps should be taken to ensure they are no longer recommended to other users. This includes content which is abusive or incites hate and is targeted at people with certain protected characteristics, and which encourages, promotes or provides instructions for suicide, self-harm and eating disorder content. As such, the removal of these suggestions is likely to have positive impacts for groups that may be disproportionately affected by such content, particularly people that share protected characteristics, who may be prompted to run searches for PPC and PC content after being presented with a predictive search suggestion, and who may be targeted by or particularly at risk of such content.

- A5.53 Measure PCS F3 recommends that providers display crisis prevention information in response to certain search requests relating to suicide, self-harm or eating disorders. It is likely to support children that are particularly vulnerable to the effects of such content, such as those with relevant protected characteristics. The measure recommends that the crisis support information displayed appears at the top of the search results, increasing the accessibility of this information, which is likely to benefit children relevant protected characteristics, for example, certain disabilities. It also recommends the information is presented and written in a manner which is understandable to children which will ensure the useability of the materials for younger users, indirectly benefitting those who may not have English as a first language or with relevant disabilities. To the extent that the measures will apply to all users of search services, the positive impacts outlined in paragraph A5.52 would be experienced by adults in addition to children.
- A5.54 We received stakeholder feedback suggesting that restricting our crisis prevention measure to search requests for suicide, self-harm and eating disorder content limited its capacity to protect other vulnerable persons or minority groups. The National Society for the Prevention of Cruelty to Children (NSPCC) expressed concern regarding our decision not to recommend crisis prevention for other kinds of PPC and PC, and said that considering the provision of supportive information for harms such as intimate image abuse and coercive and controlling behaviour only in future VAWG guidance would downgrade those measures.²⁶³ Similarly, Nexus NI suggested that we extend this measure to “sexual abuse content, domestic abuse content, content containing or pertaining to violence against women and girls, and content containing or pertaining to racism, ableism, homophobia [and] transphobia.”²⁶⁴ We recognise the need to ensure appropriate protections for individuals sharing protected characteristics associated with these harms areas. We considered this feedback in Section 19, and decided not to extend our crisis prevention measure at this stage on proportionality grounds, due to the evidence of search requests that indicate children may be in immediate need of crisis prevention information and support. This is in line with our duties under the Act. We do not consider that this measure, by not addressing the additional harms areas suggested by stakeholders, contributes to discrimination, harassment or victimisation of children with the protected characteristics associated with those harms.
- A5.55 We also received stakeholder feedback related to appropriate crisis support services for persons living in different parts of the UK. The Scottish Government suggested that “for searches within Scotland related to self-harm and general mental health and wellbeing

²⁶³ NSPCC response to May 2024 Consultation, pp.72-73.

²⁶⁴ Nexus NI response to May 2024 Consultation, pp.11-12.

support for children and young people, the Self-Harm Network Scotland and Aye Feel would be reputable websites to signpost to.”²⁶⁵

- A5.56 While we did not consider it appropriate to recommend signposting to nation-specific resources, we have clarified that the helpline provided in line with Measure PCS F3 be available 24/7, irrespective of the age or location of the user within the UK. This should have a positive impact for vulnerable children across the UK, as providers will signpost to crisis prevention helplines that are available to children irrespective of their location or remoteness in the UK.

Welsh Language Legal Framework

- A5.57 The Welsh language has official status in Wales. To give effect to this, certain public bodies, including Ofcom, are required to comply with Welsh language standards.²⁶⁶
- A5.58 The Welsh Language (Wales) Measure 2011 made the Welsh language an officially recognised language in Wales. This legislation also led to the establishment of the Office of the Welsh Language Commissioner who regulates and monitors our work. Ofcom is required to take Welsh language considerations into account when formulating, reviewing or revising policies which are relevant to Wales (including proposals which are not targeted at Wales specifically but are of interest across the UK).²⁶⁷
- A5.59 Accordingly, we have considered:
- A5.60 the potential impact of our policies on opportunities for children to use the Welsh language;
- A5.61 the potential impact of our policies on treating the Welsh language no less favourably than the English language; and
- A5.62 how our policies could be formulated so as to have, or increase, a positive impact, or not to have adverse effects or to decrease any adverse effects.

Welsh Language Impact Assessment

Our position at consultation

- A5.63 In line with the requirements listed in paragraph A5.1 to A5.5, we explained at consultation that our powers and duties in relation to online safety regulation are set out in the Act and must be exercised in accordance with our general duties under section 3 of the 2003 Act.
- A5.64 We explained that in formulating the draft Codes, where relevant and to the extent we have discretion to do so in the exercise of our functions, we considered the potential impacts on opportunities for children to use the Welsh language. We provisionally concluded they were likely to have positive effects or increased positive effects on

²⁶⁵ Scottish Government response to May 2024 Consultation, p.19.

²⁶⁶ The [Welsh language standards](#) with which Ofcom is required to comply are available on our website.

²⁶⁷ See Standards 84-89 of [Hysbysiad cydymffurfio](#) (in Welsh) and [compliance notice](#) (in English). Section 7 of the Welsh Language Commissioner’s [Good Practice Advice Document](#) provides further advice and information on how bodies must comply with the Welsh Language Standards.

opportunities to use the Welsh language and treating the Welsh language no less favourably than English.

Summary of stakeholder feedback

- A5.65 ACT - the App Association and Veridas Digital Authentication Solutions both supported our Welsh language assessment.²⁶⁸
- A5.66 We received stakeholder feedback that we should consider languages other than English and highlighted the risk that lesser used languages can be used to bypass content moderation measures.²⁶⁹ Open Rights Group and the Welsh Government both raised concerns about the impacts of the Codes on Welsh language speakers. Open Rights Group suggested that the ability to use Welsh language within the commercial settings of service moderation systems was likely to be poor or absent. The Welsh Government expressed concerns that Welsh language services would only have a small number of users, meaning they would be in scope of fewer measures, which “could in turn, unintentionally, make Welsh-speaking children more vulnerable”.
- A5.67 We also received feedback from the Welsh Government agreeing with our Welsh Language impact assessment and that the measures should have positive impacts for use of the Welsh language. They did however also query whether user support information, reporting and complaints processes and general engagement with providers would be available in a user’s preferred language, including Welsh.²⁷⁰

Our final assessment

- A5.68 We have confirmed that services should have regard to the needs of their UK user base when considering what languages are needed to effectively resource their content moderation, complaints handling, terms of service and publicly available statements.
- A5.69 In response to concerns from stakeholders about the likely size of Welsh language services and how this could affect children’s experiences online, we note that most of the measures we recommend apply regardless of a service’s size – either to all services or to services with certain risks and functionalities. The Children’s Risk Assessment Guidance is clear that small services can be risky. As such, we do not anticipate materially different outcomes for Welsh-speaking children in relation to other children in the UK.
- A5.70 In response to feedback from the Welsh Government, we note that our user support measures recommend that information and materials are clear, comprehensible and easy for a child user to understand. Inherent to this, providers should consider how information and materials can be made comprehensible to their user base, including in relation to users’ ages, abilities and language. In relation to reporting and complaints, on both user-to-user and search services, all users and affected persons should be able to make complaints about content or search content harmful to children or about the provider not complying with their duties. We also acknowledge that different groups of children may have different needs when making complaints and that this can impact upon their ability to make a complaint. This is true of language, as well as other characteristics such as ability.

²⁶⁸ ACT – The App Association response to May 2024 Consultation, p.26; Veridas response to May 2024 Consultation, p.23.

²⁶⁹ Ofcom’s Advisory Committee for Wales response to May 2024 Consultation, p.3.

²⁷⁰ Welsh Government response to May 2024 Consultation, pp.10, 12, 16.

A5.71 As such, we conclude the measures are likely to have positive effects or increased positive effects on opportunities to use the Welsh language and treating the Welsh language no less favourably than English.

A6. Additional measures suggested by stakeholders

Introduction

- A6.1 In response to our May 2024 Consultation on Protecting Children from Harms Online (May 2024 Consultation), many stakeholders provided suggestions for additional measures to be included in the Protection of Children Codes (the Codes).
- A6.2 We want to thank the large number of stakeholders who have taken the time to engage with our consultation and provide their feedback and suggestions. This annex provides an overview of their suggested additional measures.
- A6.3 Where stakeholders made suggestions that had implications for the proposed measures and analysis we set out in our May 2024 Consultation, we also discuss those suggestions in the relevant sections of Volume 4 of this statement. Where stakeholders made suggestions for new measures not directly connected to those we proposed in our May 2024 consultation, we only discuss these in this Annex. We have not assessed them for inclusion in the first version of the Codes.
- A6.4 To include any additional measures in this iteration of the Codes, beyond those we consulted on in our May 2024 Consultation, we would need to carry out additional impact assessments and a further consultation akin to the process that has informed this statement. To inform such work, we would need to assess, among other relevant considerations, whether potential additional measures fall within scope of what we can recommend in the Codes given the parameters of the Act and the evidence we have for the measures' effectiveness at addressing risks to children.
- A6.5 As discussed in Section 9, the measures that we have decided to include in this statement will deliver a significantly safer environment for children online. Our strategy is to move quickly with the publication of this first iteration of the Codes, to prevent a delay in protections for children online. However, we recognise that this is only the first step. We will be closely monitoring how service providers implement the measures in the Codes, as well as the wider package of protections for children. This will enable us to identify any gaps in protections for children, to inform our prioritisation of future work to strengthen this first set of measures.
- A6.6 We expect to consult on updating the Codes over time as we gather further information, including evidence on emerging risks to children, and explore potential new measures to keep them safe online. In Section 9 (Volume 4) of this statement, we discuss our next consultation that we will publish in the coming months. As part of any future work, we will consider additional measures suggested by stakeholders as relevant and appropriate and seek up-to-date views from stakeholders through future consultations.

Summary of stakeholder feedback

Governance and accountability

- A6.7 Several stakeholders suggested that the Codes should recommend providers gather feedback from parents, children and experts on the effectiveness of their mitigations, support information and/or tools.²⁷¹
- A6.8 The Commissioner Designate for Victims of Crime Northern Ireland suggested the Codes recommend providers proactively engage and collaborate where appropriate with child safety organisations to assist them in their governance in relation to children’s safety.²⁷²
- A6.9 Online Safety Act Network (OSA Network) called for the Codes to include measures for providers to devise appropriate metrics for monitoring the effectiveness of measures and to feed those back into their risk assessments.²⁷³
- A6.10 UK Safer Internet Centre (UKSIC) suggested that the Codes should recommend an independent auditor ensures risk assessment and governance processes are impartial.²⁷⁴
- A6.11 Smartphone Free Childhood called for the Codes to recommend service providers record information such as number of breaches and complaints, in their reporting to Ofcom.²⁷⁵
- A6.12 OSA Network called for the Codes to include “decisions taken on mitigating measures, as part of the product design process or as a response to issues arising from the risk assessment, should be recorded”.²⁷⁶
- A6.13 One individual suggested the Codes could recommend that providers in scope attend training from Ofcom on Governance, to achieve uniformity in understanding.²⁷⁷

Terms of service and publicly available statements

- A6.14 5Rights Foundation suggested the Codes should recommend providers include minimum age requirements in their terms of service and called for providers to publish which features and content they consider age appropriate for children in different age groups and what protections they have in place for those children.²⁷⁸
- A6.15 5Rights Foundation also suggested that the Codes should include measures around policies governing livestreaming, such as policies requiring adults to supervise children’s livestreams, and policies prohibiting livestreaming featuring children in bedrooms, classrooms and bathrooms.²⁷⁹
- A6.16 Internet Society and Internet Society UK England Chapter suggested a further measure for providers to include clear information in their Terms of Service on privacy enhancing technologies like end-to-end encryption (E2EE), for example instructions for use, or information about third-party access or client-side scanning.²⁸⁰

²⁷¹ Commissioner Designate for Victims of Crime Northern Ireland response to May 2024 Consultation on Protecting Children from Harms Online (May 2024 Consultation), p.6; Office of the Children’s Commissioner for England response to May 2024 Consultation, p.25; Parenting Focus response to May 2024 Consultation, p.14.

²⁷² Commissioner Designate for Victims of Crime Northern Ireland response to May 2024 Consultation, p.4.

²⁷³ Online Safety Act Network (OSA Network) (1) response to May 2024 Consultation, p.76.

²⁷⁴ UK Safer Internet Centre (UKSIC) response to May 2024 Consultation, p.7.

²⁷⁵ Smartphone Free Childhood response to the May 2024 Consultation, p.6.

²⁷⁶ OSA Network (1) response to May 2024 Consultation, p.26.

²⁷⁷ Dean, J. response to May 2024 Consultation, p.9.

²⁷⁸ 5Rights Foundation response to May 2024 Consultation, pp.3, 13-15.

²⁷⁹ 5Rights Foundation response to May 2024 Consultation, pp.7-8.

²⁸⁰ Internet Society and Internet Society UK England Chapter response to May 2024 Consultation, p.16.

Age assurance

- A6.17 Many stakeholders suggested that the Codes recommend providers use highly effective age assurance to apply their minimum age requirements.²⁸¹
- A6.18 Numerous stakeholders called for measures for providers to implement highly effective age assurance to provide age-appropriate experiences for children in different age groups.²⁸²
- A6.19 5Rights Foundation called for the Codes to recommend providers implement highly effective age assurance to mitigate the risk posed to children by the functionality of livestreaming, including through restricting viewing access and disabling the ability to host livestreams for all children or children in certain age groups.²⁸³
- A6.20 The Office of the Children’s Commissioner for England suggested that the Codes should include a direction for providers to publish in their Children’s Risk Assessment their assessment of the risk that children might circumvent age assurance measures, and to share publicly the steps taken to mitigate it.²⁸⁴
- A6.21 The Office of the Children’s Commissioner for England also called for measures for providers to take steps to prevent children encountering PPC on their services by implementing age checks at the three points of: when users access the service, when they create an account, and when they attempt to access a part of the service hosting PPC.²⁸⁵
- A6.22 The Northern Ireland Commissioner for Children and Young People (NICCY) called for the Codes to recommend that providers use age assurance to set 3-hour time limits for under 16s using social media apps.²⁸⁶
- A6.23 International Justice Mission (IJM) suggested that the Codes recommend providers explore the technological feasibility of detecting behaviour changes that might indicate a child using an adult profile.²⁸⁷

Content moderation for user-to-user services

²⁸¹ 5Rights Foundation response to May 2024 Consultation, pp.13-15; Age Verification Providers Association response to May 2024 Consultation, pp.8-10; Internet Matters response to May 2024 Consultation, pp.11-12; Islington Headteacher Network (2) response to May 2024 Consultation, p.2; Marie Collins Foundation response to May 2024 Consultation, pp.1-2; Office of the Children’s Commissioner for England response to May 2024 Consultation, pp.54, 57; Parenting Focus response to May 2024 Consultation, p.7; Vodafone response to May 2024 Consultation, p.2; Yoti response to May 2024 Consultation, p.3.

²⁸² 5Rights Foundation response to May 2024 Consultation, p.4; Barnardo’s response to May 2024 Consultation, p.26; Centre for Excellence for Children’s Care and Protection (CELCIS) response to May 2024 Consultation, p.13; Internet Matters response to May 2024 Consultation, p.11; Marie Collins Foundation response to May 2024 Consultation, p.2; National Society for the Prevention of Cruelty to Children (NSPCC) response to May 2024 Consultation, p.45.

²⁸³ 5Rights Foundation response to May 2024 Consultation, p.7.

²⁸⁴ Office of the Children’s Commissioner for England response to May 2024 Consultation, p.55.

²⁸⁵ Office of the Children’s Commissioner for England response to May 2024 Consultation, p.56.

²⁸⁶ Northern Ireland Commissioner for Children and Young People (NICCY) response to May 2024 Consultation, p.31.

²⁸⁷ International Justice Mission (IJM) response to May 2024 Consultation, p.10.

- A6.24 Many stakeholders called for the Codes to recommend automated content moderation measures.²⁸⁸ This included suggestions that we should recommend proactive detection of harmful content.²⁸⁹
- A6.25 Several stakeholders called for measures to address the risks associated with hashtags.²⁹⁰
- A6.26 National Society for the Prevention of Cruelty to Children (NSPCC) suggested measures recommending that providers should moderate users’ accounts, not just content, and called for measures that ensure that where a user with multiple accounts has one account reported, all their accounts are then blocked. It suggested that the Codes recommend providers ensure there are clear consequences for users who share harmful or dangerous content, for example, by downranking a user’s profile.²⁹¹
- A6.27 NSPCC also called for moderation measures recommending providers filter direct messaging requests to prevent users seeing requests with offensive words; to ensure “harmful content with less views and so less complaints” doesn’t “go under the radar”; to automatically hide comments which are similar to others that have been reported and to apply content warnings and blur potentially sensitive content.²⁹²
- A6.28 Some stakeholders suggested that the Codes should require providers to address harmful content in languages other than English.²⁹³
- A6.29 Conscious Advertising Network argued that the Codes should recommend content moderation measures for deepfakes.²⁹⁴
- A6.30 NSPCC suggested that the Codes should recommend providers quality assure their moderation systems and adjust the balance between human and automated moderation to ensure correct outcomes.²⁹⁵

²⁸⁸ Canadian Centre for Child Protection (C3P) response to May 2024 Consultation, pp.18-19, 21; Children and Young People’s Commissioner Scotland response to May 2024 Consultation, p.8; Christian Action Research and Education (CARE) response to May 2024 Consultation, p.5; Conscious Advertising Network and Middleton K., University of Portsmouth response to May 2024 Consultation, pp.8-9; Nexus response to May 2024 Consultation, p.15; NSPCC response to May 2024 Consultation, pp.48, 62; Office of the Children’s Commissioner for England response to May 2024 Consultation, p.47; OSA Network (1) response to May 2024 Consultation, p.73; Parenting Focus response to May 2024 Consultation, pp.36-37; UKSIC response to May 2024 Consultation, p.34; Violence Against Women and Girls (VAWG) Sector Experts, p.12.

²⁸⁹ Amaran, M. response to May 2024 Consultation, p.3; Centre to End All Sexual Exploitation (CEASE) response to May 2024 Consultation, p.17; Commissioner Designate for Victims of Crime Northern Ireland response to May 2024 Consultation, p.5; Conscious Advertising Network and Middleton K., University of Portsmouth response to May 2024 Consultation, p.27; Google response to May 2024 Consultation, p.23; National Crime Agency (NCA) response to May 2024, p.9; Vodafone response to May 2024 Consultation, p.2.

²⁹⁰ Center for Countering Digital Hate (CCDH) response to May 2024 Consultation, p.6; Molly Rose Foundation response to May 2024 Consultation, p.43; Office of the Children’s Commissioner for England response to May 2024 Consultation, pp.38-39; OSA Network (1) response to May 2024 Consultation, p.53.

²⁹¹ NSPCC response to May 2024 Consultation, pp.34, 47.

²⁹² NSPCC response to May 2024 Consultation, pp.35, 47-49.

²⁹³ Conscious Advertising Network and Middleton K., University of Portsmouth response to May 2024 Consultation, p.9; Ofcom’s Advisory Committee for Wales response to May 2024 Consultation, p.2; Open Rights Group response to May 2024 Consultation, p.17; Welsh Government response to May 2024 Consultation, p.16.

²⁹⁴ Conscious Advertising Network and Middleton K., University of Portsmouth response to May 2024 Consultation, p.20.

²⁹⁵ NSPCC response to May 2024 Consultation, p.48.

- A6.31 The Children and Young People’s Commissioner Scotland suggested the Codes should recommend the use of ‘white lists’ to categorise content from recognised sources, such as mental health charities.²⁹⁶
- A6.32 An individual called for the Codes to include a ‘buffer period’ for providers where they carry out extra checks on content to ensure it is not PPC or PC before allowing it to be viewable by the public.²⁹⁷

Search moderation, features, functionalities and user support

- A6.33 xHamster suggested measures for search services to downrank or remove search results from adult sites that do not have age assurance.²⁹⁸
- A6.34 Several stakeholders suggested measures for search services in relation to Generative Artificial Intelligence (GenAI).²⁹⁹ Microsoft suggested metaprompts and classifiers for GenAI, and citations in information returned by GenAI.³⁰⁰ NSPCC called for providers to clearly label AI-generated content in search functions (where generative AI is integrated into the search function) and include clear warnings regarding AI hallucinations and the potential for misinformation. NSPCC also suggested that GenAI functionalities should only be integrated into search functions if they are able to comply with our Search Moderation measures.³⁰¹
- A6.35 Molly Rose Foundation called for the Codes to recommend search services have the same approach to age assurance as user-to-user providers.³⁰²
- A6.36 The Office of the Children’s Commissioner for England called for the Codes to recommend safety measures to prevent harm on search services, including predictive search, personalised search, business models, commercial size or profile.³⁰³
- A6.37 Bandio called for search services to default to “appropriate for < 13 year olds” and for users who can demonstrate they are 13+ to get access to the full search engine functionality.³⁰⁴
- A6.38 Nexus and the NSPCC called for the crisis prevention measure for search services (PCS F3) to include additional harms beyond suicide, self-harm and eating disorders.³⁰⁵ Nexus’ suggestions of additional kinds of content to cover included “sexual abuse content” and content related to racism and homophobia.³⁰⁶

User reporting and complaints

²⁹⁶ Children and Young People’s Commissioner Scotland response to May 2024 Consultation, p.8.

²⁹⁷ Dean, J. response to May 2024 Consultation, p.19.

²⁹⁸ xHamster response to May 2024 Consultation, p.14.

²⁹⁹ Common Sense Media response to May 2024 Consultation, pp.4-6.

³⁰⁰ Microsoft response to May 2024 Consultation, p.13.

³⁰¹ NSPCC response to May 2024 Consultation, p.53.

³⁰² Molly Rose Foundation response to May 2024 Consultation, p.42.

³⁰³ Office of the Children’s Commissioner for England response to May 2024 Consultation, pp.38-39.

³⁰⁴ Bandio response to May 2024 Consultation, p.5.

³⁰⁵ NSPCC response to May 2024 Consultation, p.70.

³⁰⁶ Nexus response to May 2024 Consultation, pp.11-12. Nexus’ suggestions also applied to Measure PCU F3 on user signposting.

- A6.39 Several stakeholders suggested the Codes should recommend providers establish trusted flaggers programmes for content harmful to children,³⁰⁷ with some suggesting trusted flaggers should have expertise in online violence against women and girls specifically.³⁰⁸
- A6.40 The National Crime Agency (NCA) called for the Codes to recommend that providers respond to complaints within a certain timeframe.³⁰⁹
- A6.41 Common Sense Media suggested that the Codes should recommend a dedicated reporting channel for GenAI content used for bullying.³¹⁰
- A6.42 Internet Matters suggested measures recommend providers to offer peer reporting tools for children and reporting mechanisms for parents and teachers.³¹¹
- A6.43 One individual indicated the Codes should recommend providers enable children to report to their parents.³¹²
- A6.44 Another individual responded that the Codes should recommend service providers enable children to share a report's progress with a linked account.³¹³
- A6.45 NICCY suggested that the Codes should recommend service providers offer a "child-friendly justice process".³¹⁴
- A6.46 Various stakeholders suggested that the Codes should recommend service providers communicate the outcomes of complaints to complainants.³¹⁵
- A6.47 The Office of the Children's Commissioner for England stated that the Codes should recommend service providers be obliged to publish reports detailing what harms have been reported and what action was taken to mitigate them. They also suggested that Ofcom set a minimum outcome standard for service providers which could be used to assess the effectiveness of services' reporting tools.³¹⁶
- A6.48 OSA Network suggested that the Codes should recommend providers collect data on or respond to patterns of complaints.³¹⁷
- A6.49 xHamster called for the Codes to recommend additional mechanisms to tackle abusive reporting to ensure the user reporting system remains effective.³¹⁸

³⁰⁷ NSPCC response to May 2024 Consultation, pp.57-58; Scottish Government response to May 2024 Consultation, p.16; UKSIC response to May 2024 Consultation, p.8.

³⁰⁸ OSA Network (1) response to May 2024 Consultation, p.75; VAWG Sector Experts response to May 2024 Consultation, p.13.

³⁰⁹ NCA response to May 2024 Consultation, p.12.

³¹⁰ Common Sense Media response to May 2024 Consultation, p.5.

³¹¹ Internet Matters response to May 2024 Consultation, p.16.

³¹² Amaran, M. response to May 2024 Consultation, p.3.

³¹³ Dean, J. response to May 2024 Consultation, p.16.

³¹⁴ NICCY response to May 2024 Consultation, p.33.

³¹⁵ CELCIS response to May 2024 Consultation, p.15; Children and Young People's Commissioner Scotland response to May 2024 Consultation, p.10; Children's Commissioner for Wales response to May 2024 Consultation, p.3; Dean, J. response to May 2024 Consultation, pp.16-17; NICCY response to May 2024 Consultation, p.34; NSPCC response to May 2024 Consultation, pp.56-57; Scottish Government response to May 2024 Consultation, p.16; Welsh Government response to May 2024 Consultation, p.12.

³¹⁶ Office of the Children's Commissioner for England response to May 2024 Consultation, p.64.

³¹⁷ OSA Network (1) response to May 2024 Consultation, p.76.

³¹⁸ xHamster response to May 2024 Consultation, p.11.

Recommender systems on user-to-user services

- A6.50 An individual called for consideration of measures for providers to potentially disable recommender algorithms for younger children and suggested that providers ‘blacklist’ any user who uploads content identified as PPC/PC so that their content is not included in recommender algorithms.³¹⁹
- A6.51 Several stakeholders suggested that the Codes should require algorithmic testing and audits.³²⁰
- A6.52 Integrity Institute suggested that the Codes should recommend providers only include content from followed accounts in recommender feeds.³²¹
- A6.53 NSPCC recommend a step be added to the Codes requiring providers to test their Recommender Systems for filtering out PPC and to monitor and report on their efficacy.³²²
- A6.54 Children and Young People’s Commissioner Scotland called for the Codes to recommend providers use ‘white lists’ to only categorise authoritative content.³²³ Similarly, [SC] suggested that the Codes recommend content should primarily come from “trusted media sources”.³²⁴
- A6.55 Conscious Advertising Network called for consideration of whether advertising pushed by algorithm should be removed from the feeds of children.³²⁵
- A6.56 NICCY recommended that the Codes require providers to publish clear information on the purposes for which algorithms are deployed, the data they are using to feed the algorithms, and the outcomes they produce (both intended and unintended consequences).³²⁶

User support and safety settings

- A6.57 NSPCC suggested the Codes recommend providers display warnings when users repeatedly attempt to post offensive comments and enable children to turn off tagging and sharing of their posts. It also called for users to be able to mute voice chat and turn off sharing their content in games and suggested that providers prompt users to reconsider their safety settings.³²⁷
- A6.58 Brave Movement and NSPCC suggested the Codes should recommend measures to tackle the risks of direct, group and encrypted messaging.³²⁸ OSA Network similarly suggested

³¹⁹ Dean, J. response to May 2024 Consultation, pp.11, 14.

³²⁰ 5Rights Foundation response to May 2024 Consultation, p.10; NCA response to May 2024 Consultation, p.6; Parenting Focus response to May 2024 Consultation, pp.10, 12, 15, 37.

³²¹ Integrity Institute response to May 2024 Consultation, p.18.

³²² NSPCC response to May 2024 Consultation, pp.61-62.

³²³ Children and Young People’s Commissioner Scotland response to May 2024 Consultation, p.8.

³²⁴ [SC]

³²⁵ Conscious Advertising Network and Middleton K., University of Portsmouth response to May 2024 Consultation, p.36.

³²⁶ NICCY response to May 2024 Consultation, p.32.

³²⁷ NSPCC response to May 2024 Consultation, pp.29, 35, 67, 69.

³²⁸ Brave Movement response to May 2024 Consultation, p.2; NSPCC response to May 2024 Consultation, pp.35-37.

measures should include ‘systemic actions’ providers could take to protect children in group chats.³²⁹

- A6.59 Snap Inc. called for the Codes to include various additional measures for group chats such as only allowing users to be invited to group chats by someone they are already friends with; users manually approving any inbound comments before they can appear publicly; users having the option to decline an invitation to join a group chat if the group includes someone they have already blocked; limiting the size of group chats; providing users with group chat reporting tools and “flagging risks or restrictions based on other factors beyond those taken only the individual user”.³³⁰
- A6.60 The Office of the Children’s Commissioner for England suggested the integration into the Codes of “a triaging function for mental health helplines”.³³¹
- A6.61 Beat indicated that the Codes should include guidelines for users who wish to create recovery-focused content to ensure they produce safe and supportive material. It also indicated that measures recommending these individuals be provided with access to mental health resources and support, rather than punitive measures, would be helpful.³³²
- A6.62 Conscious Advertising Network suggested that the Codes recommend providers issue tailored support mechanisms for vulnerable children and those with Special Educational Needs and Disabilities.³³³
- A6.63 [X] also suggested that the Codes recommend providers offer free user verification for all users, so that it is easier for users to know who they’re interacting with.³³⁴
- A6.64 Internet Matters called for the Codes to include prevention messages for bullying and harassment to tackle child-on-child harm.³³⁵ NSPCC argued that “alongside proactive content moderation, services should utilise other tools and functionalities to prevent and minimise the impact of bullying and harassment.”³³⁶
- A6.65 5Rights Foundation suggested that the Codes should recommend providers issue warning messages to children when they have been contacted by suspected bad actors, or, where possible, prevent them from contacting children at all.³³⁷
- A6.66 Integrity Institute called for measures to include other controls for users, such as for limiting content from accounts they don’t follow, limiting direct messages or comments from unknown or anonymous accounts, and having settings private by default. They also suggested that measures should include interventions to teach and remind users of the tools.³³⁸

Other suggestions

³²⁹ OSA Network (1) response to May 2024 Consultation, pp.53-54.

³³⁰ Snap Inc. response to May 2024 Consultation, pp.25-26.

³³¹ Office of the Children’s Commissioner for England response to May 2024 Consultation, pp.74-75.

³³² Beat response to May 2024 Consultation, p.3.

³³³ Conscious Advertising Network and Middleton K., University of Portsmouth response to May 2024 Consultation, p.11.

³³⁴ [X]

³³⁵ Internet Matters response to May 2024 Consultation, p.16.

³³⁶ NSPCC response to May 2024 Consultation, p.35.

³³⁷ 5Rights Foundation response to May 2024 Consultation, p.8.

³³⁸ Integrity Institute response to May 2024 Consultation, p.19.

- A6.67 Many stakeholders suggested the Codes should include parental controls measures.³³⁹
- A6.68 Samaritans called for the introduction of measures to mitigate the increasing level of content being used to make money.³⁴⁰
- A6.69 The Office of the Children’s Commissioner for England recommended the Codes should include measures to address features designed to maximise the length of time children spend on a service.³⁴¹ 5Rights Foundation recommended that “persuasive design” and addictive features should be redesigned, for example by imposing ‘timeouts’ or changing the design of children’s feeds.³⁴²
- A6.70 OSA Network and NSPCC suggested the Codes recommend providers should be required to address addictive design and features that maintain high engagement, such as ‘likes’, ‘streaks’ and endless scrolling. They alternatively suggested these functionalities should be turned off by default for children.³⁴³
- A6.71 Some stakeholders suggested measures specifically for livestreaming.³⁴⁴
- A6.72 The Office of the Children’s Commissioner for England suggested the Codes should include measures that providers assess the “motivation behind the design of any feature or functionality of an online service, and the impact that it will have on the interests of children”.³⁴⁵
- A6.73 Several stakeholders suggested that the Codes should recommend that age inappropriate or ‘risky’ features, such as livestreaming, should be disabled until a mitigation is identified.³⁴⁶

³³⁹ Amaran, M. response to May 2024 Consultation, p.5; Apple response to May 2024 Consultation, p.3; Big Brother Watch response to May 2024 Consultation, p.3; Conscious Advertising Network and Middleton K., University of Portsmouth response to May 2024 Consultation, pp.6, 17; Dean, J. response to May 2024 Consultation, p.11; East Riding of Yorkshire Council response to May 2024 Consultation, p.2; Family Online Safety Institute (FOSI) response to May 2024 Consultation, pp.7-8; Google response to May 2024 Consultation, p.23; Individual anonymous 1 response to May 2024 Consultation, p.1; Internet Matters response to May 2024 Consultation, pp.3, 10; Kidify response to May 2024 Consultation, pp.3, 5; Meta Platforms Inc. response to May 2024 Consultation, p.30; [§<]; National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) response to May 2024 Consultation, p.21; Northeastern University London response to May 2024 Consultation, pp.2-3; Office of the Children’s Commissioner for England response to May 2024 Consultation, pp.49-50; Parenting Focus response to May 2024 Consultation, pp.6, 10; Scottish Government response to May 2024 Consultation, pp.12, 19; Smartphone Free Childhood response to May 2024 Consultation, p.7; Snap Inc. response to May 2024 Consultation, pp.12, 25-26; Vodafone response to May 2024 Consultation, p.1.

³⁴⁰ Samaritans response to May 2024 Consultation, p.9.

³⁴¹ Office of the Children’s Commissioner for England response to May 2024 Consultation, p.48.

³⁴² 5Rights Foundation response to May 2024 Consultation, p.10.

³⁴³ NSPCC response to May 2024 Consultation, p.18; OSA Network (1) response to May 2024 Consultation, pp.35-37.

³⁴⁴ 5Rights Foundation response to May 2024, pp.7-8; Internet Watch Foundation (IWF) response to May 2024 Consultation, p.4; Molly Rose Foundation response to May 2024 Consultation, p.43; Office of the Children’s Commissioner for England response to May 2024 Consultation, p.38; UKSIC response to May 2024 Consultation, p.22.

³⁴⁵ Office of the Children’s Commissioner for England response to May 2024 Consultation, pp.70-71.

³⁴⁶ 5Rights Foundation, pp.7-8; Global Action Plan response to May 2024 Consultation, pp.1-2; UKSIC response to May 2024 Consultation, p.22.

- A6.74 Several stakeholders suggested that the Codes recommend providers limit, and in some cases disable, certain features/functionalities for contacting children.³⁴⁷ Some suggested, for example, that providers should prevent children being added or invited to group chats.³⁴⁸ Conscious Advertising Network also called for children to be prevented from accessing encrypted services, suggesting that at the very least children should only be accessing encrypted services and engaging in group chats with individuals they know, such as verified friends and family. They also suggested that services should ensure children are not able to see or make comments on strangers' content.³⁴⁹
- A6.75 The Office of the Children's Commissioner for England, the Molly Rose Foundation and OSA Network called for measures to address the risks associated with the following: group messaging, direct messaging, ephemeral messaging.³⁵⁰ Brave Movement recommended "robust measures for private messaging",³⁵¹ and 5Rights Foundation suggested that private messaging, ephemeral messaging, and private attachments in messages should be disabled for all children or children in certain age groups.³⁵²
- A6.76 Integrity Institute recommended measures on enhanced privacy controls and defaults, for example, to limit direct messages or comments from unknown or anonymous accounts,³⁵³ and the Scottish Government recommended that services should be required to have settings set as private by default for children.³⁵⁴
- A6.77 Lucy Faithfull Foundation called for the Codes to recommend that providers introduce friction for adult users attempting to contact children³⁵⁵ and 5Rights Foundation suggested adult users should be prevented from sending unsolicited friend requests to U18s if this activates direct messaging.³⁵⁶ Canadian Centre for Child Protection (C3P) stated that services should ensure that children are uncontactable by other users.³⁵⁷
- A6.78 OSA Network and VAWG Sector Experts called for measures to address the risks associated with stranger pairing.³⁵⁸

³⁴⁷ Conscious Advertising Network and Middleton, K., University of Portsmouth response to May 2024 Consultation, p.15; Molly Rose Foundation response to May 2024 Consultation, p.13; OSA Network response to May 2024 Consultation, p.3.

³⁴⁸ Commissioner Designate for Victims of Crime Northern Ireland response to May 2024 Consultation, p.5; Conscious Advertising Network and Middleton K., University of Portsmouth response to May 2024 Consultation, p.25; OSA Network (1) response to May 2024 Consultation, p.54.

³⁴⁹ Conscious Advertising Network and Middleton K., University of Portsmouth response to May 2024 Consultation, pp.15, 25.

³⁵⁰ Molly Rose Foundation response to May 2024 Consultation, p.43; Office of the Children's Commissioner for England response to May 2024 Consultation, p.39; OSA Network (1) response to May 2024 Consultation, p.53.

³⁵¹ Brave Movement response to May 2024 Consultation, p.3.

³⁵² 5Rights Foundation response to May 2024 Consultation, p.8.

³⁵³ Integrity Institute response to May 2024 Consultation, p.19.

³⁵⁴ Scottish Government response to May 2024 Consultation, p.19.

³⁵⁵ Lucy Faithfull Foundation provided example of adult users sending invitations to group chats to large volumes of children, particularly children with whom they have no connection. Lucy Faithfull Foundation response to May 2024 Consultation, p.3.

³⁵⁶ 5Rights Foundation response to May 2024 Consultation, p.8.

³⁵⁷ C3P response to May 2024 Consultation, p.30.

³⁵⁸ OSA Network (1) response to May 2024 Consultation, p.53; VAWG Sector Experts response to May 2024 Consultation, p.11.

- A6.79 Several stakeholders recommended the Codes should address multiple/fake accounts.³⁵⁹ For example, UKSIC suggested that measures recommend that providers prevent the creation of fake profiles.³⁶⁰
- A6.80 The Office of the Children’s Commissioner for England and OSA Network called for measures to address the risks associated with anonymous profiles.³⁶¹
- A6.81 OSA Network also suggested measures in relation to location information on livestreaming.³⁶²
- A6.82 Various stakeholders raised that the Codes should include measures to combat the risks to children posed by AI generated content.³⁶³ NSPCC called for measures for deepfake technology, often used for cyberbullying.³⁶⁴
- A6.83 The Office of the Children’s Commissioner for England called for measures relating to reposting, resharing and forwarding content, hyperlinks, posting multimedia, screenshotting or recording; user tagging; user profiles; user connections; user groups; encrypted messaging; fake accounts, user location and editing tools. They also suggested the inclusion of safety measures in relation to functionalities “after harm occurs on search services”.³⁶⁵
- A6.84 Several stakeholders suggested that the Codes should recommend product testing.³⁶⁶ The Office of the Children’s Commissioner for England called for measures to recommend providers complete a child risk assessment during the product testing phase of technological development.³⁶⁷
- A6.85 TikTok suggested that we should “amend the Code such that they facilitate the continued testing of new systems, for example through the application of a Good Samaritan principle, or a regulatory sandbox model.”³⁶⁸
- A6.86 OSA Network suggested additional Codes measures in areas including “design of functionalities, algorithms and other features”, to include product testing and monitoring and measurement (of the effectiveness of measures).³⁶⁹
- A6.87 Integrity Institute called for measures to recommend providers analyse and report why people, particularly children, are exposed to violating content.³⁷⁰

³⁵⁹ NSPCC response to May 2024 Consultation, pp.33-34; OSA Network (1) response to May 2024 Consultation, p.23; VAWG Sector Experts response to May 2024 Consultation, p.11.

³⁶⁰ UKSIC response to May 2024 Consultation, p.43.

³⁶¹ Office of the Children’s Commissioner for England response to May 2024 Consultation, p.39; OSA Network (1) response to May 2024 Consultation, p.53.

³⁶² OSA Network (2) response to May 2024 Consultation, pp.8-9.

³⁶³ NSPCC response to May 2024 Consultation, pp.12-15; OSA Network (1) response to May 2024 Consultation, pp.13-15, 54-56; Parenting Focus response to May 2024 Consultation, pp.9-10.

³⁶⁴ NSPCC response to May 2024 Consultation, p.14.

³⁶⁵ Office of the Children’s Commissioner for England response to May 2024 Consultation, pp.38-39.

³⁶⁶ Molly Rose Foundation response to May 2024 Consultation, pp.12-13; OSA Network (1) response to May 2024 Consultation, pp.24, 26; Samaritans response to May 2024 Consultation, p.4.

³⁶⁷ Office of the Children’s Commissioner for England response to May 2024 Consultation, p.62.

³⁶⁸ TikTok response to May 2024 Consultation, p.6.

³⁶⁹ OSA Network (1) response to May 2024 Consultation, pp.3-4, 26.

³⁷⁰ Integrity Institute response to May 2024 Consultation, pp.17-18.

- A6.88 The Children and Young People’s Commissioner Scotland, VAWG Sector Experts and Beat suggested there should be measures to improve and support children’s access to good quality information.³⁷¹ VAWG Sector Experts added that measures should ensure access remained to information in relation to issues surrounding gender, sexual education or reproductive rights.³⁷² Beat indicated that safe information and resources relating to eating disorders should remain accessible.³⁷³
- A6.89 Several stakeholders suggested that the Codes recommend Media Literacy interventions.³⁷⁴
- A6.90 Several stakeholders called for the Codes to recommend providers consult with children and young people directly on issues related to online harms.³⁷⁵ In addition to this, OSA Network suggested that services should have a requirement to take action/make modifications to the way their service is operating based on feedback from children.³⁷⁶
- A6.91 A few stakeholders suggested that the Codes should include an alternative dispute resolution (ADR).³⁷⁷
- A6.92 NICCY called for the Codes to include limiting access to the sale of harmful products.³⁷⁸

³⁷¹ Beat response to May 2024 Consultation, p.3; Children and Young People’s Commissioner Scotland response to May 2024 Consultation, pp.3-6; VAWG Sector Experts response to May 2024 Consultation, p.7.

³⁷² VAWG Sector Experts response to May 2024 Consultation, p.7.

³⁷³ Beat response to May 2024 Consultation, p.3.

³⁷⁴ Commissioner Designate for Victims of Crime Northern Ireland response to May 2024 Consultation, p.2; Common Sense Media response to May 2024 Consultation, p.6; Conscious Advertising Network and Middleton K., University of Portsmouth response to May 2024 Consultation, p.7; Internet Matters response to May 2024 Consultation, p.17; VAWG Sector Experts response to May 2024 Consultation, pp.13, 15.

³⁷⁵ Barnardo’s response to May 2024 Consultation, p.25; Office of the Children’s Commissioner for England response to May 2024 Consultation, p.6; Scottish Government response to May 2024 Consultation, p.11.

³⁷⁶ OSA Network (1) response to May 2024 Consultation, p.53.

³⁷⁷ Trust Alliance Group (TAG) response to May 2024 Consultation, p.3; UKSIC response to May 2024 Consultation, pp.4-5, 9.

³⁷⁸ NICCY response to May 2024 Consultation, p.26.

A7. Glossary

This glossary defines the terms we have used throughout the statement.

| Term | Definition |
|---|---|
| 2003 Act | The Communications Act 2003 (c.21). |
| 2020 Video-Sharing Platform Regulation Call for Evidence | <i>‘Video-sharing platform regulation Call for Evidence’</i> , published by Ofcom on 16 July 2020 , available at Call for evidence: Video-sharing platform regulation |
| 2022 Illegal Harms Call for Evidence | <i>‘First phase of online safety regulation Call for Evidence’</i> , published by Ofcom on 6 July 2022, available at Call for evidence: First phase of online safety regulation |
| November 2023 Illegal Harms Consultation | <i>‘Consultation: Protecting people from illegal harms online’</i> , published by Ofcom on 9 November 2023, available at Consultation: Protecting people from illegal harms online |
| 2023 Protection of Children Call for Evidence | <i>‘Second phase of online safety regulation Call for Evidence’</i> , published by Ofcom on 10 January 2023, available at Call for evidence: Second phase of online safety regulation |
| Abuse and hate content | Content, described in section 62(2) of the Act, which is abusive and which targets any of the following characteristics— (a) race, (b) religion, (c) sex, (d) sexual orientation, (e) disability, or (f) gender reassignment and/or content, described in section 62(3) of the Act, which incites hatred against people— (a) of a particular race, religion, sex or sexual orientation, (b) who have a disability, or (c) who have the characteristic of gender reassignment. |
| Access control | Technical mechanism which prevents users who have not been age assured, or having been age assured, did not meet the requirements of the age assurance process, from accessing a service (or part of it) or certain content. |
| Act | The Online Safety Act 2023 . |
| Age appropriate user support materials | Materials that are specifically designed to be accessible and understandable to all children permitted to use a service, and to the adults who care for them. |
| Age assurance | A collective term for age verification and age estimation. |
| Age assurance method | The particular system or technology that underpins an age assurance process. |
| Age assurance process | 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. |
| Age assurance report | The Act requires Ofcom to produce a report about the use of age assurance, assessing how providers of regulated services have used age assurance for the purpose of compliance with their duties, how effective the use of age assurance has been for that purpose, and |

| | |
|--|--|
| | whether there are factors that have prevented or hindered the effective use of age assurance. ³⁷⁹ |
| Age-check | An individual instance of an age assurance process being applied to a user. |
| Age estimation | A form of age assurance designed to estimate the age or age range of the user. ³⁸⁰ |
| Age verification | A form of age assurance designed to verify the exact age of the user. ³⁸¹ |
| Algorithm speak (algospeak) | Coded language used online in order to circumvent content moderation methods. This could also include the use of emojis. |
| Anonymous user profiles | User-to-user service functionality allowing users to create a user profile where their identity ³⁸² is unknown to an extent. This includes instances where a user's identity is unknown to other users; for example, through the use of aliases (pseudonymity). It also includes where a user's identity may be unknown to a service, for example, services that do not require users to register by creating an account. |
| Autoplay features | Feature that allows audiovisual content to continue playing without input from the user. |
| Avatar research methodology | Research methodology involving accounts or profiles set up on online services by researchers, modelled on the behaviours and interests of real users. |
| Blocking | A user-to-user functionality where: a) blocked users cannot send direct messages to the blocking user and vice versa; b) the blocking user will not encounter any content posted by blocked users on the service and vice versa; c) the blocking user and blocked user, if they were connected, will no longer be connected. |
| Blurring, distorting or obscuring | Any action that means that the content cannot be clearly seen by users. For example, this may be done by a greyscale overlaying an image, accompanied by a content warning. |
| Bot | An umbrella term that refers to a software application or automated tool which has been programmed to carry out a specific or predefined task without any human intervention. |
| Business models | The way in which a business operates to achieve its goals. For the purposes of the Children's Register of Risks, this includes a service's revenue model and growth strategy. |
| Chatbot | A computer program designed to simulate a conversation with human users, typically through typed text in a software application. They can be powered by artificial intelligence (AI) techniques, or by rule-based systems and predefined scripts. |

³⁷⁹ Section 157 of the Act.

³⁸⁰ Section 230(3) of the Act.

³⁸¹ Section 230(2) of the Act.

³⁸² Identity refers to an individual's formal or officially recognised identity.

| | |
|---|--|
| Characteristic | In respect of a regulated service, includes references to its functionalities, user base, business models, governance, and other systems and processes. ³⁸³ |
| Child | A person under the age of 18. |
| Child user | A user under the age of 18. |
| Children’s Access Assessments Guidance | Guidance for Part 3 services on children’s access assessments, available at Children’s access assessments . |
| Children’s code | The ICO’s Children’s code (also known as the Age Appropriate Design code). ³⁸⁴ |
| Children’s Register of Risks | The assessment of the risks of harm to children from content harmful to children on user-to-user and search services that Ofcom is required to prepare under section 98 of the Act, available at Children’s Register of Risks . |
| Children’s risk assessment | The most recent children’s risk assessment carried out by the provider, pursuant to sections 11 and 28 of the Act. |
| Children’s Risk Profiles | Prepared under section 98 of the Act and as set out in Part 3 of the Children’s Risk Assessment Guidance . |
| Children’s safety duties | The safety duties protecting children in sections 12 and 29 of the Act. |
| Clear web | Publicly accessible websites that are indexed by search engines. |
| Codes of practice (Codes) | The sets of measures recommended by Ofcom for compliance with the children’s safety duties, in accordance with section 41 of the Act, available at Protection of Children Code of practice for user-to-user services and Protection of Children Code of practice for search services . |
| Combined service | A regulated user-to-user service that includes a public search engine. ³⁸⁵ |
| Combining visual media | User-to-user functionality that allows users to join together videos and/or images, often from different sources, into one piece of content that can be shared. |
| Commenting on content | User-to-user service functionality that allows users to reply to content, or post content in response to another piece of content posted on open channels of communication, visually accessible directly from the original content without navigating away from that content. |
| Commercial profile | The size of the service in terms of capacity, ³⁸⁶ the stage of service maturity and rate of growth in relation to users or revenue. |
| Community | Also referred to as “groups” or “forum groups”, where a user-to-user service functionality allowing users to create online spaces that are often devoted to sharing content on a particular topic. User groups can be open |

³⁸³ Section 98(11) of the Act.

³⁸⁴ ICO. [Age appropriate design: a code of practice for online services | ICO](#). [accessed 30 April 2024].

³⁸⁵ Section 4(7) of the Act.

³⁸⁶ In terms of number of employees and/or revenue.

| | |
|------------------------------------|--|
| | to the public or closed to the public, requiring a registered account and an invitation or approval from existing members to gain access. |
| Content audience | Refers to whether content is shared on open or closed channels of communication. Open channels are areas of services where content is visible to the general public or any user. Closed channels are areas of a service where content is limited to a smaller audience, and where users can expect more privacy, such as direct messaging or user groups that have controls or restrictions on who can join. |
| Content controls | A means of restricting certain user's access to a particular piece of content on a service. |
| Content editing | Functionality type that comprises user-to-user functionalities which allow users to alter user-generated content before or after it is shared. |
| Content exploring | Functionality type that comprises user-to-user functionalities which allow users to explore and search for user-generated content. |
| Content format | Refers to the format in which content is made available. This, for instance, includes content in the form of images, video, audio, text and emojis. |
| Content recommender systems | An algorithmic system which determines the relative ranking of an identified pool of content (that includes regulated user generated content) from multiple users on content feeds. Content is recommended based on factors that it is programmed to account for, such as popularity of content, characteristics of a user, or predicted engagement. References to content recommender systems do not include a content recommender system employed exclusively in the operation of a search functionality which suggests content to users in direct response to a search query, product recommender systems or network recommender systems. |
| Content restriction tools | <p>User tools that allow users to privately (i.e., not visible to any other user of the service, including the creator of the content) restrict their interaction with a piece of content or kind of content, so that less or none of that content appears on their content feed in future. In some cases, the user may still be able to access the content if they search for it directly.</p> <p>These tools have different names on different services. Examples we are aware of include 'see less of this' and 'hide' tools. We would not consider a 'dislike' button to be a content restriction tool, if its primary function is to publicly express an opinion about the content rather than to restrict interaction with it. However, a 'not interested' button might be a content restriction tool if its primary function is to allow users to privately restrict interaction with a piece or kind of content.</p> |

| | |
|---|---|
| Content storage and capture | Functionality type that comprises user-to-user functionalities that allow users to record and store user-generated content. |
| Content tagging | User-to-user service functionality allowing users to assign a keyword or term to content that is shared. |
| Content | Anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description. ³⁸⁷ |
| Crisis prevention information | Refers to information provided by a search service in search results that typically contains the contact details of helplines and/or links to supportive information provided by a reputable organisation, to assist users experiencing a mental health crisis. |
| CSAM (child sexual abuse material) | A category of illegal CSEA content, including in particular indecent or prohibited images of children (including still and animated images, and videos, and including photographs, pseudo-photographs and non-photographic images such as drawings). CSAM also includes other material that includes advice about grooming or abusing a child sexually or which is an obscene article encouraging the commission of other child sexual exploitation and abuse offences; content which links or otherwise directs users to such material; or content which advertises the distribution or showing of CSAM. |
| CSEA (child sexual exploitation and abuse) | Refers to offences specified in Schedule 6 of the Act, including offences related to CSAM and grooming. CSEA includes but is not limited to causing or enticing a child or young person to take part in sexual activities, sexual communication with a child and the possession or distribution of indecent images. |
| Cumulative harm | Harm that occurs when harmful content (PPC, PC or NDC) is repeatedly encountered by a child, and/or when a child encounters harmful combinations of content. These combinations of content include encountering different types of harmful content (PPC, PC or NDC), or a type of harmful content (PPC, PC, or NDC) alongside a kind of content that increases the risk of harm from PPC, PC or NDC. ³⁸⁸ |
| Dangerous stunts and challenges content | Content which encourages, promotes, or provides instructions for a challenge or stunt highly likely to result in serious injury to the person who does it or to someone else. |
| Dating services | User-to-user service type describing services that enable users to find and communicate with romantic or sexual partners. |

³⁸⁷ Section 236 of the Act.

³⁸⁸ Section 234(4) of the OS Act.

| | |
|---|--|
| December 2024 Illegal Harms Statement | <i>‘Protecting people from illegal harms online’</i> , published by Ofcom on 16 December 2024, available at Statement: Protecting people from illegal harms online . |
| Dedicated Reporting Channel (DRC) | A means for a Trusted Flagger (defined below) to report problems, for example an inbox, a web portal or another relevant mechanism for reporting. |
| Deepfake | A form of audio-visual content that has been generated or manipulated using AI, and that misrepresents someone or something. Deepfakes are usually intended to cause harm by deceiving an audience into believing that something happened when it did not. In some cases, deepfakes consist of wholly new content, whereas in others they take the form of existing content that has been manipulated in some way. |
| Direct messaging | User-to-user service functionality allowing a user to send and receive a message to one recipient at a time, and which can only be immediately viewed by that specific recipient. |
| Discussion forums and chat room services | A user-to-user service type describing general services that generally allow users to send or post messages that can be read by the public or an open group of people. |
| Downranking | Action taken by a search service which involves altering the ranking algorithm such that a particular piece of search content appears lower in the search results and is therefore less discoverable to users |
| Downstream general search service | Search service type describing a subsection of general search services. Downstream general search services provide access to content from across the web, but they are distinct in that they obtain or supplement their search index from other general search services. |
| Doxxing | The intentional online exposure of an individual’s identity, private information or personal details without their consent. ³⁸⁹ |
| Eating disorder content | Content which encourages, promotes or provides instructions for an eating disorder or behaviours associated with an eating disorder. ³⁹⁰ |
| Editing visual media | User-to-user service functionality that allows users to alter or manipulate images, videos or computer-generated media by means of the service. |
| Ephemeral messaging | User-to-user service functionality that allows users to send messages that are automatically deleted after they are viewed by the recipient, or after a prescribed period of time has elapsed. |
| Explicit feedback | Direct and intentional actions taken by users to express their preferences and sentiment on content. Though it can vary across services; explicit feedback into recommender systems can be positive (such as likes or saves) or negative (such as dislikes or clicking ‘show me less’ or reporting the content). Depending on the |

³⁸⁹ eSafety Commissioner, 2020. [What is doxing or doxxing?](#) [accessed 18 April 2024].

³⁹⁰ Section 61(5) of the Act.

| | |
|---|---|
| | service, user reports or complaints can also be forms of explicit negative feedback. |
| External content policies | Publicly available documents aimed at users of the service which provide an overview of a service's rules about what content is allowed and what is not. These are often in the form of terms of service and/or community guidelines. |
| Extreme pornography | An umbrella term to cover several categories of images which are illegal to possess, broadly covering images which are produced principally for sexual arousal, and which depict extreme or obscene behaviours. ³⁹¹ |
| File-storage and file-sharing services | User-to-user service type describing services whose primary functionalities involve enabling users to store digital content and share access to that content through links. |
| Filter bubble | Where a user experiences a narrowing of the type or nature of content they encounter on an online service, typically on a U2U service. This can result in increasing content homogeneity and a relative reduction in content variety. Filter bubbles are typically algorithmically driven but may be caused by other factors that limit a user's exposure to content that is thematically varied. |
| Filtering | Action taken by the provider of a search service to ensure that certain items of content do not appear in search results or recommendation feeds based on whether a condition is met/is not met. For example, ensuring that identified PPC is not returned in search results of relevant users, or content that is indicated potentially to be PPC is excluded from recommender feeds. |
| Functionalities | <p>In relation to a user-to-user service, includes any feature that enables interactions of any description between users of the service by means of the service.³⁹²</p> <p>In relation to a search service, includes (in particular): (a) a feature that enables users to search websites or databases; (b) a feature that makes suggestions relating to users' search requests (predictive search functionality).³⁹³</p> <p>In practice, when referring to functionalities in the Register of Risks, 'functionalities' refers to the front-end features of a service. For user-to-user services, 'functionalities' refers to features that enable interaction between users. 'Functionalities for search services' refers to features that enable users to search</p> |

³⁹¹ Defined in section 63 of the Criminal Justice and Immigration Act 2008 (c.4).

³⁹² Section 233(1) of the Act. Please refer to section 233(2) of the OS Act for a non-comprehensive list of user-to-user functionalities.

³⁹³ Section 233(3) of the OS Act.

| | |
|---|--|
| | websites or databases, as well as features that make suggestions relating to users' search requests. |
| Fundraising services | User-to-user service type describing services that typically enable users to create fundraising campaigns and collect donations from users. |
| Gaming services | User-to-user service type describing services that allow users to interact within partially or fully simulated virtual environments. |
| General search services | Search service type describing services that enables users to search the internet and which derives search results from an underlying search index (developed by either the service or a third party). |
| Generative artificial intelligence (GenAI) | AI models that can create text, images, audio and videos, typically in response to a user prompt. |
| Governance | Structures that ensure the adequate oversight, accountability, and transparency of decisions within a service which affect user safety. This is in relation to organisational structure as well as product and content governance. |
| Grooming | An offence under paragraphs 5, 6, 11 or 12 of Schedule 6 to the Act. |
| Group messaging | User-to-user service functionality allowing users to send and receive messages through a closed channel of communication to more than one recipient at a time. |
| Harm | Means physical or psychological harm. References to harm presented by content, and any other reference to harm in relation to content, have the same meaning given to it by section 234 of the Act. |
| Harmful substances content | Content which encourages a person to ingest, inject, inhale or in any other way self-administer (a) a physically harmful substance, or (b) a substance in such a quantity as to be physically harmful. |
| Hate offences | Public order offences relating to stirring up hatred on the grounds of certain protected characteristics. |
| High-capacity services | Services with a large number of employees and/or revenue. ³⁹⁴ |
| Highly effective age assurance | An age assurance process that is of such a kind and implemented in such a way that it is highly effective at correctly determining whether or not a particular user is a child. |
| Hyperlinking | Functionality providing direct access to another piece of data by clicking or tapping on specific content present on the service. |
| Illegal content | Content that amounts to a relevant offence. |
| Illegal harm | Harms arising from illegal content and the commission and facilitation of priority offences. |
| Image or video search | Search service functionality that allows users to search for images and/or videos. |

³⁹⁴ Our evidence does not currently allow for quantitative thresholds to be drawn for service capacity. Services should nevertheless consider the number of employees and revenue as a risk factor.

| | |
|---|--|
| Immersive technology | Technologies that create and enhance a sense of presence when interacting digitally with content and other users. |
| Implicit feedback | Techniques used to infer user preferences from observations and data available to a recommender system. This can include user actions such as page views, clicking, and hovering over content. Implicit feedback may be used as proxy for positive engagement that may not always be intended by users, and they may not be aware that it's being collected. |
| Indexing | Process of collecting, parsing, and storing of data by a search engine to facilitate fast and accurate information retrieval. |
| Infinite scrolling | A design pattern in which a page loads content as a user scrolls down, allowing them to discover and view large amounts of content with no distinct end. This design pattern is typically associated with content recommender system where large volumes of personalised content is curated. |
| Information-sharing services | User-to-user service type describing services that are primarily focused on providing user-generated informational resources to other users. |
| Internal content policies | More detailed versions of external content policies which set out rules, standards or guidelines, including around what content is allowed and what is not, as well as providing a framework for how policies should be operationalised and enforced. |
| January 2025 Statement | <i>'Statement: Age Assurance and Children's Access'</i> , published by Ofcom on 16 January 2024, available at Statement: Age Assurance and Children's Access . |
| Large service | A service with more than 7 million monthly active UK users. |
| Leet speak | Leet speak or 'l337 speak' refers to an informal online language where numbers or special characters are used to replace vowels or consonants. |
| Livestreaming | User-to-user service functionality that allows users to simultaneously create and broadcast online streaming media in, or very close to, real time. |
| Low-risk service | A service which the provider has not assessed as being medium or high risk in relation to any kind of content harmful to children in its risk assessment. |
| Marketplaces and listings services | User-to-user service type describing services that allow users to buy and sell their goods or services. |
| May 2024 Consultation | <i>'Consultation: Protecting children from harms online'</i> , published by Ofcom on 8 May 2024, available at Consultation: Protecting children from harms online . |
| 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 underestimation. 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 $MAE = (1/n) \sum_{i=1}^n$ |

| | |
|---|--|
| | $ y - x $ where n = number of observations in the dataset, y = is the true value, x = is the predicted value. |
| Meme | A form of content, such as an image or video, that is spread widely on the internet, often altered by internet users for humorous effect. ³⁹⁵ |
| Messaging services | User-to-user service type describing services that are typically centred around the sending and receiving of messages that can only be viewed or read by a specific recipient or group of people. |
| Micro-businesses | Businesses that employ 1-9 full-time employees. |
| Moderation | When a service provider reviews and assesses content to determine whether it is harmful to children or not, or whether it is in breach of the terms of service or publicly available statement of the service, and takes appropriate action based on that determination We use 'content moderation' when referring to U2U services, and 'search moderation' when referring to search services. |
| Multi-risk service | A service is multi-risk if the provider has assessed the service as having medium or high risk of two or more specific kinds of content that is harmful to children. |
| Muting | Muting refers to a feature that enables a user to 'mute' another user. The muting user will not encounter any content posted by muted users on the service (unless the muting user visits the user profile of the muted user directly). The muted user is not aware that they have been muted and continues to encounter content posted by the muting user. |
| Negative feedback | Data and signals that indicate a user's dissatisfaction or lack of interest in a content recommendation. Examples include data or signals from reporting processes and content restriction tools. |
| Non-designated content | Content, which is not Primary priority content or Priority content, of a kind which presents a material risk of significant harm to an appreciable number of children in the UK. ³⁹⁶ |
| Overlays or interstitials | Elements such as pop-ups or webpages which appear before the target content is displayed, or while navigating between pages. Typically, the user will need to take an action, such as clicking through, to reach the target content. |
| Part 3 HEAA Guidance | 'Guidance on highly effective age assurance for Part 3 services', available at Guidance on highly effective age assurance . |
| Part 3 or regulated search service | Refers to a search service that falls within the definition of section 4 of the Act. |
| Part 3 or regulated user-to-user service | A user-to-user service, as defined in section 4 of the Act. |

³⁹⁵ [Collins Dictionary](#). [accessed 18 April 2024].

³⁹⁶ Section 60(2)(c) of the Act.

| | |
|--|--|
| Pile-on | Refers to when a user is criticised or targeted by a large number of other users, often as part of bullying campaigns. |
| Pornography services | Services whose principal purpose is the hosting or dissemination of pornographic content and who host user-generated pornographic content. These services are subject to the risk assessment duties and the children's safety duties. Pornography that is published or displayed by the provider of the service is subject to different duties set out in Part 5 of the Act and Ofcom has published separate guidance for providers subject to these duties. |
| Posting content | User-to-user service functionality allowing users to upload and share content on open channels of communication. |
| Posting goods or services for sale | User-to-user service functionality allowing users to post content dedicated to offering goods and services for sale. This does not include paid-for advertisements, but may serve the function of allowing users to promote goods or services. ³⁹⁷ |
| Posting or sending location information | User-to-user service functionality allowing users to share their current or historic location, record a user's movement, or identify which other users of the service are nearby. |
| Predictive search | An algorithmic functionality embedded in the search field of a search service. It operates by anticipating a user's search query and suggesting possible related search requests ('predictive search suggestions'), based on a variety of factors (including a user's past queries and other user queries, locations, and trends) to help users make more relevant searches. |
| Primary priority content | A category of content that is harmful to children, as defined in section 61 of the Act. ³⁹⁸ |
| Priority content | A category of content that is harmful to children, as defined in section 62 of the Act. ³⁹⁹ |
| Priority offences | Offences set out in Schedules 5 (Terrorism offences), 6 (CSEA offences) and 7 (Priority offences) to the Act. |
| Proactive technology | Content identification technology, user profiling technology, and behaviour identification technology (subject to certain exceptions) as defined in section 231 of the Act. |
| Protected characteristics | Age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; and sexual orientation. ⁴⁰⁰ |

³⁹⁷ See 'advertising-based revenue model' in business models for more information.

³⁹⁸ We have typically grouped the different kinds of primary priority content as follows: pornographic content, suicide and self-harm content, eating disorder content. This reflects the definition in section 61 of the Act.

³⁹⁹ We have typically grouped the different kinds of priority content as follows: abuse and hate content, bullying content, violent content, harmful substances content, dangerous stunts and challenges content. This reflects the definition in section 62 of the Act.

⁴⁰⁰ Section 4 of the Equality Act 2010.

| | |
|---|--|
| Publicly available statement | A statement that search services are required to make available to members of the public in the UK, often detailing various information on how the service operates. |
| Rabbit hole | The process of recommending ever more extreme content to users over time, which may occur as a result of users engaging with that type of content in the past. ⁴⁰¹ |
| Reacting to content | User-to-user service functionality allowing users to express a reaction, such as approval or disapproval, of content that is shared by other users, through dedicated features that can be clicked or tapped by users. ⁴⁰² |
| Record keeping and review guidance | The guidance that Ofcom is required to produce under section 52(3) of the Act to help services to comply with their record keeping and review duties under sections 23 (U2U) and 34 (search) of the Act, available at Record-Keeping and Review Guidance . |
| Reposting or forwarding content | User-to-user service functionality which allows users to re-share content that has already been shared by a user. |
| Revenue model | How a service generates income or revenue. |
| Review service | A service which enables users to create and view reviews of people, businesses, products, or services. |
| Risk assessment | Identifying and assessing the risk of harm to individuals from illegal content and content harmful to children, present on a Part 3 regulated service. |
| Risk factor | A characteristic associated with the risk of one or more kinds of harm. |
| Risk of harm | The possibility of individuals encountering harm on a Part 3 service. |
| Safe search | A feature of several general search services which filters or blurs certain kinds of search content, such as pornographic/sexual or violent content. Search services can have different levels of safe search settings, and users can typically opt in or out of them. In some cases, a safe search setting is enabled by default by a service, for example for children or for user accounts in educational institutions. |
| Screen capturing or recording | User-to-user service functionality that allows users to capture an image or record a video showing the contents of their display. ⁴⁰³ |
| Search content | Content that may be encountered in or via search results of a search service. It does not include paid-for advertisements, news publisher content, or content |

⁴⁰¹ PATTRN.AI, 2023. [Evaluating recommender systems in relation to the dissemination of illegal and harmful content in the UK](#) [accessed 22 April 2024].

⁴⁰² This for instance includes ‘liking’ or ‘disliking’ a post.

⁴⁰³ While users can often record or capture content using third-party services, screen recordings and captures are often shared on user-to-user services as user-generated content and some user-to-user services have dedicated screen recording and screen capturing functionalities.

| | |
|--|---|
| | that reproduces, links to, or is a recording of, news publisher content. |
| Search engine | Includes a service or functionality which enables a person to search some websites or databases but does not include a service which enables a person to search just one website database. ⁴⁰⁴ |
| Search index | A collection of URLs that are obtained by deploying crawlers to find content across the web, which is subsequently stored and organised. |
| Search query inputs | Search service functionality type by means of which users input search queries. |
| Search result | In relation to a search service, this means content presented to a user of the service by operation of the search engine, in response to a search query made by a user. ⁴⁰⁵ |
| Search services | An internet service that is, or includes, a search engine. |
| Self-declaration (age) | A process where the user is asked to provide their own age. This could be in the form of providing a date of birth to gain entry to a service or by ticking a box to confirm a user is over a minimum age threshold. |
| Service | A regulated user-to-user or search service. |
| Service design | The design of all the components that shape a user's end-to-end experience of a service. These components can include the business model or decision-making structures, back-end systems and processes, the user interface, and off-platform interventions. |
| Service type | A characteristic that in general refers to the nature of the service. For example, social media services and messaging services. ⁴⁰⁶ |
| Small business | A business that employs 10-49 full-time employees. |
| Social media services | User-to-user service type describing services that connect users and enable them to build communities around common interests or connections. |
| Stories | Feature on some services that allows users to post images and videos that are ephemeral. |
| Stranger pairing | User-to-user functionality that allows users to be matched with other users of the service who they may not know to facilitate user-to-user interaction. |
| Subscription-based revenue models | Revenue models that generate income by selling access (or premium access) to a service for a period of time in return for a fee. |
| Suicide and self-harm content | Content which encourages, promotes or provides instructions for suicide or encourages, promotes or provides instructions for an act of deliberate self-injury. |
| Systems and processes | Characteristic concerning the actions taken by a service, including procedures to mitigate the risk of children being harmed by encountering content that is harmful |

⁴⁰⁴ Section 229(1) of the Act.

⁴⁰⁵ Section 57(3) of the Act.

⁴⁰⁶ Certain service types have been selected because our evidence suggests that they play a role in children encountering harmful content.

| | |
|---------------------------------------|---|
| | to them. This can be either human or automated, or a combination of the two, and include technology. |
| Terms of Service | All documents comprising the contract for use of the service (or of part of it) by UK users. |
| Trolling | When someone posts or comments online to deliberately upset others. ⁴⁰⁷ |
| Trusted flagger | A person with expertise relating to one or more types of harm to children for whom the provider has established a dedicated reporting channel. |
| URL (Uniform Resource Locator) | A reference that specifies the location of a resource accessible by means of the internet. |
| User access | A user's entry into a service and ability to use the functionalities present on that service. |
| User base demographics | Demographic make-up of the user base, including selected characteristics, intersectional dynamics and other relevant demographic factors. |
| User base | Users of a service. A user does not need to be registered with a service to be considered a user of that service. ⁴⁰⁸ |
| User communication | Functionality type that comprises user-to-user service functionalities which allow users to communicate with one another, either synchronously or asynchronously. Includes communication across open and closed channels. ⁴⁰⁹ |
| User connections | User-to-user service functionality that allows users to follow or subscribe to other users. Users must sometimes be connected in order to view all or some of the content that each user shares. |
| User feedback | The various types of user data and signals collected by recommender systems to learn about their preferences and make predictions about what content is likely to be relevant. This feedback helps content recommender systems personalise content suggestions. User feedback can take a variety of forms and can be explicit and implicit, which we have defined separately. |
| User groups | User-to-user service functionality allowing users to create online spaces that are often devoted to sharing content on a particular topic. User groups are generally closed to the public and require an invitation or approval from existing members to gain access. However, in some cases they may be open to the public. |
| User identification | Functionality type that comprises user-to-user service functionalities which allow users to identify themselves to other users. |
| User networking | Functionality type that comprises user-to-user service functionalities which allow users to find or encounter each other, and establish contact. |

⁴⁰⁷ eSafety Commissioner, 2024. [Trolling | What does trolling mean?](#) [accessed 18 April 2024].

⁴⁰⁸ Section 227 of the OS Act makes clear that 'it does not matter whether a person is registered to use a service' for them to be considered a 'user.'

⁴⁰⁹ See content audiences for definition of open and closed channels of communication.

| | |
|---|---|
| User profiles | User-to-user service functionality that is associated with a user account, that represents a collection of information shared by a user which may be viewed by other users of the service. This can include information such as username, biography, profile picture, etc., as well as user-generated content generated, shared or uploaded by the user using the relevant account. ⁴¹⁰ |
| User report | User reports are a specific type of complaint about content, submitted through a reporting tool. |
| User tagging | User-to-user service functionality allowing users to assign other users, typically by their username, to content that is shared. |
| User-generated content | Content (a) that is (i) generated directly on the service by a user of the service, or (ii) uploaded to or shared on the service by a user of the service; and (b) which may be encountered by another user, or other users, of the service by means of the service. |
| User-generated content searching | User-to-user service functionality allowing users to search for user-generated content by means of a user-to-user service. |
| User-to-user services | An internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service. |
| Vent post | Content that is typically posed by a user to express personal problems or challenges. |
| Vertical search services | Search service type describing services that enable users to search for specific topics, or products or services (e.g. flights or hotels) offered by third-party operators. Unlike general search services, they do not return search results based on an underlying search index. Rather, they may use an API or equivalent technical means to directly query selected websites or databases with which they have a contract, and to return search results to users. |
| Video-sharing services | User-to-user service type describing services that allow users to upload and share videos with the public. |
| Violent content | Content which encourages, promotes or provides instructions for an act of serious violence against a person or animal. ⁴¹¹ |
| Virality | The degree to which online content spreads easily and/or quickly across many online users, alongside how much engagement and/or views a piece of content received (i.e., 'shares', 'likes', and 'views', etc.). |

⁴¹⁰ Users can sometimes create fake user profiles, which are not a functionality in themselves, but are user profiles that impersonates another entity or are intentionally misleading.

⁴¹¹ Content which— (a) depicts real or realistic serious violence against a person; (b) depicts the real or realistic serious injury of a person in graphic detail. Content which— (a) depicts real or realistic serious violence against an animal; (b) depicts the real or realistic serious injury of an animal in graphic detail; (c) realistically depicts serious violence against a fictional creature or the serious injury of a fictional creature in graphic detail. Defined by Section 62(6) and 62(7) of the Act.

| | |
|--------------------------------------|--|
| Virtual private network (VPN) | The creation of a private network over a public internet connection. |
|--------------------------------------|--|