

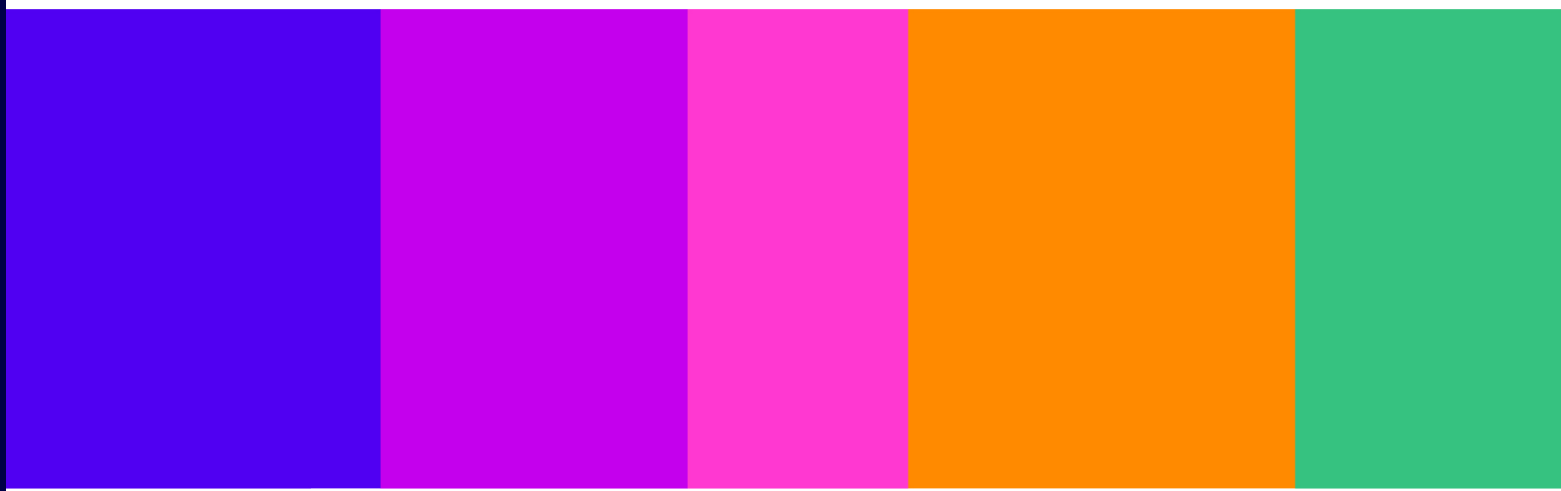
# Protecting children from harms online

---

A summary of our consultation

[Welsh version available](#)

Published 8 May 2024



# Contents

---

## Section

|                              |    |
|------------------------------|----|
| Overview .....               | 3  |
| What we are proposing .....  | 6  |
| What we have published ..... | 25 |

# Overview

**This document is a summary of Ofcom’s consultation on protecting children online. It is designed to be a summary of our proposals to help interested parties review them quickly. Please read the full consultation documents where you require more comprehensive information.**

The UK Online Safety Act 2023 (‘the Act’) makes platforms – including social media, search, and pornography services – legally responsible for keeping people, especially children, safe online. These services have new duties to protect users in the UK by assessing risks of harm and taking steps to address them. As the UK’s online safety regulator, Ofcom’s role is to provide codes and guidance to support regulated services to comply with their duties and deliver a safer life online for people in the UK. The online safety regime is hugely ambitious, and as laid out in our [roadmap](#), we are moving fast to implement these new laws.

Securing a higher level of protection online for children than adults is one of the objectives of the Act. This objective runs through the policies we have proposed in prior consultations. In our [Illegal Harms Consultation](#), we set out proposals to protect children from illegal content and activity, including contact harms like grooming, as well as child sexual exploitation and abuse. In our [Part 5 Consultation](#), we proposed how online providers of pornographic content should prevent children from accessing pornographic content.

Building on these earlier consultations, here we put forward a comprehensive set of draft codes and guidance that will support online services in better protecting children. These proposals reflect what we know from available research and evidence about risks to children, including what children themselves have told us.

Children benefit from the opportunities that technology offers and enjoy being online for learning, friendships, and entertainment. But our assessment of the causes and impacts of harm to children shows us that most have encountered harmful content and activity online, with serious impact on their physical and mental wellbeing. Occasionally online activity is also linked to fatal outcomes.

## What online services must do to protect children

**Assess whether children are likely to access their service – or part of it.** This involves completing “children’s access assessments”. We have published [draft Children’s Access Assessments Guidance](#) designed to help service providers comply. We anticipate that most services not using highly effective age assurance are likely to be accessed by children within the meaning of the Act. Those that are likely to be accessed by children must then complete the following steps.

**Complete a children’s risk assessment to identify risks their service(s) pose to children.** This is known as the “children’s risk assessment”. Children’s risk assessments are separate to the illegal content risk assessments that all services need to complete. We have published [draft Children’s Risk Assessment Guidance](#). This step-by-step guidance explains how services can complete the assessment and assess the risks to children. It also includes our draft Children’s Risk Profiles, providing an overview of factors that increase the risks of harm to children, which services must consult in carrying out their children’s risk assessment.

Services must prevent children from encountering the most harmful content relating to suicide, self-harm, eating disorders, and pornography. Services must also minimise children’s exposure to other serious harms, including violent, hateful or abusive material, bullying content, and content promoting dangerous challenges.

Our [draft Children's Register of Risks](#) provides more information on how risks of harm to children manifest online; and our [draft Guidance on Content Harmful to Children](#) sets out examples of what Ofcom considers to be content harmful to children.

**Take and implement safety measures to mitigate the risks to children.** We are proposing more than 40 safety measures in our draft Children's Safety Codes for [user-to-user](#) and [search services](#), in these broad areas:

- **Robust age checks.** We expect much greater use of age assurance, so services know which of their users are children. All services which do not ban harmful content, and those at higher risk of it being shared on their service, should implement highly effective age-checks to prevent children from seeing it.
- **Safer algorithms.** Recommender systems – algorithms which provide personalised recommendations to users – are children's main pathway to harm online. Under our proposals, any service which operates a recommender system and is at higher risk of harmful content should identify who their child users are and configure their algorithms to filter out the most harmful content from children's feeds and reduce the visibility of other harmful content.
- **Effective moderation.** All user-to-user services should have content moderation systems and processes that ensure swift action is taken against content harmful to children. Search services should also have appropriate moderation systems and, where large search services believe a user to be a child, a 'safe search' setting which children should not be able to turn off should filter out the most harmful content.
- **Strong governance and accountability.** Proposed measures here include having a named person as accountable for compliance with the children's safety duties; an annual senior-body review of all risk management activities relating to children's safety; and an employee Code of Conduct that sets standards for employees around protecting children.
- **More choice and support for children.** This includes ensuring clear and accessible information for children and carers, with easy-to-use reporting and complaints processes, and giving children tools and support to help them stay safe.

**We expect these measures to make a big difference to children's online experiences.** For example:

- Children will not normally be able to access pornography.
- Children will be protected from seeing, and being recommended, potentially harmful content.
- Children will not be added to group chats without their consent.
- It will be easier for children to complain when they see harmful content, and they can be more confident that their complaints will be acted on.

We explain our proposals in brief in this document and our [Proposed Codes at a glance](#) provides an overview of the measures we are proposing in our draft Codes.

**Keep children's access assessments, children's risk assessments, and safety measures under review.** Services that are not 'likely to be accessed by children' need to carry out children's access assessments annually, and before any major changes to their services. And services need to keep their children's risk assessments up to date, including when Ofcom makes significant changes to the Children's Risk Profiles, and before making any significant changes to their design and operation. We also suggest that service providers monitor the effectiveness of the safety measures they take or implement, and continually improve them over time.

## Measures need to be proportionate

The Act requires us to ensure our proposals are proportionate. The primary consideration in designing our proposals is the extent to which they can reduce risks to children, having regard to the need for a higher level of protection for children than for adults.

We recognise that the size, capacity, and risks of services differ widely, and we therefore do not take a one-size-fits-all approach. Instead, we have set out what types of service we think should use specific safety measures to comply with their duties, with the most extensive expectations on the riskiest services.

Services cannot decline to take steps to protect children merely because it is too expensive or inconvenient – protecting children is a priority and all services, even the smallest, will have to take action as a result of our proposals.

The measures proposed in this consultation will necessarily have an impact on the experiences of children and adults and can impact their rights to freedom of expression and other fundamental rights. We have sought to ensure that our measures will protect children online without unduly affecting user rights or undermining innovation and investment in high-quality online services that children and adults benefit from.

## Updating our codes and guidance

This is the first version of our regulatory guidance and codes relating to protecting children. We expect to update these products over time as new evidence arises on emerging risks to children and what measures will best keep children safe online. We have already identified some areas where we want to explore complementary measures, including in relation to the use of automated content moderation to detect illegal and harmful content, as we discuss in [Volume 5](#).

## Next steps

We are inviting stakeholder responses to our consultation by 17 July 2024. We will take all feedback into account, as well as engaging with children to hear what they think of our plans. We expect to finalise our proposals and publish our final statement and documents in spring 2025.

# What we are proposing

This is an overview of our consultation on protecting children from harm online. It is a high-level summary of what we are proposing to help interested parties quickly get to grips with our proposals.

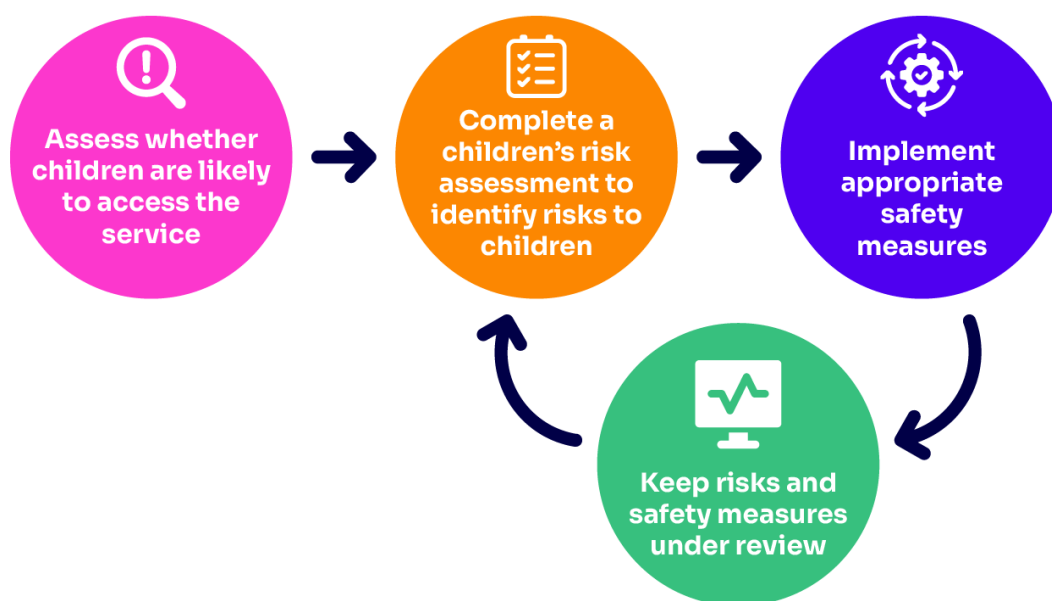
The full detail of our proposals and the reasoning behind them, as well as detailed consultation questions, are set out in the full consultation document. Please read the full consultation documents if you require more comprehensive information.

## Protecting children online

The Act creates a new regulatory framework which aims to make the online world safer for people in the UK. Securing better protections to help keep children safer online is one of the Act's main objectives. The Act is clear that the duties imposed on regulated services aim to make sure they are safe by design, and designed and operated in a way that provides a higher standard of protection for children than for adults.

The Act sets out requirements for user-to-user services and search services to ensure they protect children online,<sup>1</sup> including:

- carrying out **children's access assessments** to assess whether children can access their service(s) or part of it;
- if appropriate, carrying out a **children's risk assessment** to assess the risks their service(s) pose to children;
- **take safety measures** to tackle risks and protect children online; and
- **keep risks and safety measures under review.**<sup>2</sup>



<sup>1</sup> Refer to Chapter 3 of [Volume 1](#) of our [Illegal Harms Consultation](#) for more information on the types of services in scope of the online safety regime.

<sup>2</sup> Refer to Scope of this consultation, Section 2, Volume 1, for more information.

## Content that is harmful to children

When complying with the children’s safety duties, service providers need to consider different types of content that is harmful to children. The Act defines ‘content that is harmful to children’ into three broad categories:<sup>3</sup>

| Category of content   | Brief description  |
|---|--|
| <b>Primary priority content that is harmful to children</b>                     | Pornographic content, and content which encourages, promotes, or provides instructions for suicide, self-harm, and eating disorders.   |
| <b>Priority content that is harmful to children</b>                             | Content which is abusive or incites hatred, bullying content, and content which encourages, promotes, or provides instructions for violence, dangerous stunts and challenges, and self-administering harmful substances. |
| <b>Non-designated content that presents a material risk of harm to children</b> | Any types of content that do not fall within the above two categories which present “a material risk of significant harm to an appreciable number of UK children”.   |

## Our draft codes and guidance

Our package of draft codes and guidance is designed to support online services in complying with their duties under the Act – and forms the foundations of services having the systems and processes to deliver safer online experiences for children. It is based on our assessment of the risks that children face online. [Volume 3](#) sets out our full analysis of the causes and impacts of harm to children online. We have also drawn together substantial input from the online sector, as well as children’s organisations, academics, independent researchers, and other public bodies.

In developing our proposals, our primary aim has been to ensure children are protected online. As required by the Act, we have also weighed up the impact and cost to services and sought to be proportionate in our proposals. And we have ensured that, where any proposed measure interferes with people’s fundamental rights, such as freedom of expression and privacy, this interference is proportionate to our objective of protecting children.<sup>4</sup>

We’ve also aimed to ensure consistency with our [Illegal Harms Consultation](#) and [Part 5 Guidance](#). We outline any key differences within this document with further detail in the relevant sections of the consultation.

**The rest of this document provides an overview of our proposals to help interested parties quickly get to grips with our proposals.**

---

<sup>3</sup> Refer to our draft Guidance on Content Harmful to Children (Volume 3, Sections 8.1-8.10).

<sup>4</sup> Refer to *What should services do to mitigate the risk of online harms to children* (Volume 5) for more information on how we have developed our proposals.

# Phase 1: Assessing whether children can access online services

---

We have published our [draft Children's Access Assessments Guidance](#) on how services should complete children's access assessments.

All providers will need to complete what is known as 'children's access assessments'. These will help services determine whether their service – or a part of it – is likely to be accessed by children.

Children's access assessments must be 'suitable and sufficient'. There are two broad stages:

- **Stage 1:** Providers must determine whether it is possible for children to access their service or part of it; and, if so, move to Stage 2.
- **Stage 2:** Whether there are significant numbers of children using the service and/or the service is likely to attract a significant number of children (the 'child user condition').

Most service providers must complete their first children's access assessments within three months of Ofcom's publishing our final children's access assessments guidance.

Our draft Children's Access Assessments Guidance – as summarised below – is aimed at helping services to complete their children's access assessments, including by setting out how to approach the assessments and what to consider at each stage. We think this process will be straightforward for most providers.

## Our proposals – in brief

### Stage 1: Is it possible for children to access the service or part of it?

Providers must decide whether it is possible for children to access their service or part of it. Providers can only conclude it is not possible for children to access the service if they are using age verification or age estimation (together known as age assurance), which prevents children from accessing that service. The age assurance used needs to be highly effective at preventing children from accessing the service or the relevant part of it.

By 'highly effective', we mean it must be technically accurate, robust, reliable, and fair. There is more detail on what constitutes highly effective age assurance in our draft guidance at [Annex 10](#). In brief, here is what each criterion means.

- **Technical accuracy** – the degree to which an age assurance method can correctly determine a user's age under test lab conditions.
- **Robustness** – the degree to which an age assurance method can correctly determine a user's age in unexpected or real-world conditions.
- **Reliability** – the degree to which the age output from an age assurance method performs in consistently producing the same or similar outputs when given the same or similar inputs.
- **Fairness** – the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.

Examples of age assurance methods that have the potential to meet the above criteria include photo-ID matching, facial age estimation, and reusable digital identity services. Examples of age assurance methods that are not capable of being highly effective include payment methods which do not require the user to be over 18, self-declaration of age, and general contractual restrictions on the use of the service by children.



If a provider has highly effective age assurance in place, they do not need to go on to complete Stage 2 of the children's access assessment. They can conclude that the service is not likely to be accessed by children and so they are not subject to the children's safety duties. Providers who conclude that their service is not likely to be accessed by children should record the evidence supporting their conclusion.

## Stage 2: Is the child user condition met?

If the provider finds that children can access the service or part of it, they should move on to Stage 2 and consider whether the 'child user condition' is met. This is the case if one or both of the following criteria is met:

- a significant number of children are using the service; and/or
- the service is of a kind likely to attract a significant number of children.

The provider must choose which criterion to consider first to establish if the child user condition is met. Service providers, especially those without reliable age assurance methods, often find it difficult to accurately distinguish between adult and child users, making it hard to determine how many children are using the service.

Providers might therefore wish to focus on the second criterion – whether the service is likely to attract a significant number of children. We have proposed a list of factors that providers should consider when making this assessment:

- whether the service provides benefits to children – such as entertainment, education, or support;
- whether the content on a service is appealing to children;
- whether the design of the service is appealing to children; and
- whether children form part of the service's commercial strategy.

Even if your service does not actively target children or seeks to limit access to children below a certain minimum age, it may still be of a kind likely to attract a significant number of children.

The Act does not define what is meant by a 'significant number' of children. This is likely to depend on the nature of the service and should reflect a number or proportion that is material in the context of the service. Even a relatively small number of children could be significant in terms of the risk of harm. We suggest service providers should err on the side of caution in making their assessment.

## Recording the outcome

Providers should record the outcome of their children's access assessment, regardless of its findings. Where providers conclude that the child user condition is not met, they should record the steps taken and the evidence used to reach this conclusion. These service providers should be prepared to demonstrate this with detailed evidence. Services that conclude they meet the child user condition do not need to record detailed evidence to back this conclusion.

Service providers may already have assessed whether they are likely to be accessed by children for the purposes of the Information Commissioner's Office (ICO) [Children's code](#) for the purposes of complying with data protection regulation, and may be able to draw on the same evidence and analysis for both.

## How to make sure children are kept safe online

---

Services that are considered likely to be accessed by children will then need to take steps to protect them:

- **Complete ‘children’s risk assessments’ to identify the risks their services pose to children.** Our draft Children’s Risk Assessment Guidance and associated documents help services complete this process.
- **Put safety measures in place to mitigate the identified risks and ensure children are protected online.** Our draft Children’s Safety Codes sets out the proposed measures in full.

## Phase 2: Completing the children’s risk assessment

---

We have published [our draft Children’s Risk Assessment Guidance on how services should complete their children’s risk assessment](#).

Services that are likely to be accessed by children will be required to complete a children’s risk assessment. This is to ensure they have an adequate understanding of the risks to children that arise from their service and implement the necessary measures to manage and mitigate those risks.

Our draft Children’s Risk Assessment Guidance is intended to help services meet their risk assessment duties and sets out the steps that services can follow to complete a suitable and sufficient risk assessment (which we summarise below). Services must also consult our draft Children’s Risk Profiles when completing their children’s risk assessment, which provide an overview of risk factors that increase the risks of harm arising from different kinds of content harmful to children.

Our [draft Children’s Register of Risks](#) sets out how risks of harm to children manifest online and our [draft Guidance on Content Harmful to Children](#) sets out examples of what kinds of content Ofcom considers to be, or not to be, content harmful to children. Both documents can also be used as reference material.

### Our proposals – in brief

We have sought to align our draft Children’s Risk Assessment Guidance with our draft Illegal Harms Risk Assessment Guidance where possible. Services likely to be accessed by children must carry out a children’s risk assessment *in addition to* their illegal harms risk assessment.

Services are required to complete a ‘suitable and sufficient’ children’s risk assessment, which has two broad elements: completing all the relevant elements of the children’s risk assessment in the Act; and carrying out each element to a suitable and sufficient standard for their service.

Our proposed approach to risk assessments is rooted in best practice relating to risk management systems. We propose that services follow a four-step methodology for their children’s risk assessment:<sup>5</sup>

- **Understand content that could be harmful to children.** Services should review the types of content that could be harmful to children as part of the risk assessment process – these are listed in the draft Risk Assessment Guidance. Our draft Guidance on Content

---

<sup>5</sup> Refer to our draft Children’s Risk Assessment Guidance, including how to use the associated draft Children’s Risk Profiles.

Harmful to Children and draft Children’s Register of Risks provide more information on this. Our draft Children’s Risk Profiles will help them identify risk factors that might apply to their service for each kind of content harmful to children.

- **Assess the risk of harm.** Services should then assess the risks of harm that children might face when they use them. To do this, they should use the risk factors they identified using the draft Children’s Risk Profiles and assess the likelihood and impact of each kind of content harmful to children. This step should also involve considering the impact of a service’s characteristics that might increase or decrease risks of harm to children – for example, how a service is used, its features and characteristics and the risk of cumulative harm. We also provide guidance on how services should assign a risk level to each relevant type of content harmful to children. This has an impact later in terms of what safety measures they should consider implementing from our Codes.
- **Implement safety measures and record outcomes.** Services should decide on the measures to reduce the risk of harm to children. The decision about which measures to implement should be informed by the risk level assigned in Step 2 and take into consideration our draft Children’s Safety Codes (outlined below).
- **Report, review and update their children’s risk assessment.** Services should report on their children’s risk assessment and measures via their governance channels (such as senior governance boards). They should also monitor the effectiveness of the safety measures put in place. Children’s risk assessments should be reviewed at specific points, including when we update our Children’s Risk Profile and before a service provider makes a significant change to the design or operation of the service. We recommend that services should also review their children’s risk assessments at least every 12 months.

More information on each step is outlined in [Volume 4](#) and [Annex 6](#).

## Phase 3: Safety measures to protect children online

---

**Our draft Children’s Safety Codes set out the safety measures [user-to-user](#) and [search services](#) can take to help keep children safe.**

Services likely to be accessed by children are required by the Act to use proportionate safety measures to keep them safe. Our draft Children’s Safety Codes provide a set of safety measures that online services can take to help them meet their duties under the Act. Services can decide to comply with their duties by taking different measures to those in the Codes. However, they will need to be able to demonstrate that they offer the appropriate level of safety for children.

Our draft Codes bring together a broad package of safety measures that aim to protect children online. They also work alongside the other pillars of the Online Safety regime to collectively improve safety online for everyone, especially children.

For example, our [draft Illegal Harms Safety Codes](#), published in November 2023, will have a positive impact on children as they set out proposed measures aimed at preventing them seeing illegal content and stopping contact from potential perpetrators of child sexual abuse and exploitation offences. And our [draft Guidance for service providers publishing pornographic content](#) will help online services that display pornography to comply with their duties to put in place highly effective age assurance measures to ensure children are not able to encounter pornography on them. We’ll

also be publishing guidance in early 2025 containing best practice for services on how they can take further steps to tackle online gendered harm against users (such as misogyny), including children.

There is no single fix-all measure that services can take to protect children online. Safety measures need to work together to help create an overall safer experience for children. We have proposed a set of safety measures within our draft Children’s Safety Codes, that will work together to achieve safer experiences for children online. These cover three broad areas:

- **robust governance and accountability** – ensuring service providers have appropriate senior oversight and accountability for children’s safety online;
- **safer platform design choices** – making sure services understand their users’ ages and keep children safe, including ensuring recommender systems and content moderation operate effectively to prevent harm to children; and
- **providing children with information, tools, and support** – ensuring service providers provide clear and accessible information to children and carers, making sure reporting and complaints functions are easy to use, and giving children tools and support to help them stay safe.

## Robust governance and accountability

Strong governance and accountability are crucial to service providers’ efforts in protecting children online. By governance and accountability, we mean the structures and processes organisations use to ensure there is adequate oversight of decision-making, roles and responsibilities, and effective reporting and review mechanisms.

We are therefore proposing measures for how service providers should approach governance and accountability in relation to protecting children online. These cover four main areas: governance arrangements; senior accountability and responsibility; internal assurance; and staff policies and training.

These complement the related guidance for providers in our draft Children’s Risk Assessment Guidance, discussed above. We think the totality of these measures will ensure there is a high level of senior oversight of how service providers are handling and mitigating risks of harm to children – and help make sure services are designed and operated in ways that effectively mitigate those risks.

Our approach is consistent with our Illegal Harms Consultation. This means service providers who must comply with both illegal content safety duties and children’s safety duties can choose to adopt a single process that covers both areas.

### Our proposals – in brief

| #   | Proposed measure  | Who should implement this <sup>6</sup>  |
|-----|---|---|
| GA1 | Most senior body to carry out and record an annual review of risk management activities relating to children’s safety | All user-to-user services that are large<br><br>All large general search services |

<sup>6</sup> In the tables throughout this section, we refer to "multi-risk". This means that we propose the measure to apply if the service has concluded it is at risk of more than one type of content harmful to children.

| #   | Proposed measure  | Who should implement this <sup>6</sup>   |
|-----|---|--|
| GA2 | Name a person accountable to most senior governance body for compliance with children’s safety duties   | All user-to-user services<br><br>All search services   |
| GA3 | Written statements of responsibility for senior members who make decisions relating to management of child safety risks   | All user-to-user services that are: <ul style="list-style-type: none"> <li>• Large, or</li> <li>• Multi-risk for content harmful to children.</li> </ul> All search services that are: <ul style="list-style-type: none"> <li>• Large general search services, or</li> <li>• Multi-risk for content harmful to children</li> </ul> |
| GA4 | Have an internal monitoring and assurance function to provide independent assurance that measures are effective   | All user-to-user services that are: <ul style="list-style-type: none"> <li>• Large; and</li> <li>• Multi-risk for content harmful to children</li> </ul> All search services that are: <ul style="list-style-type: none"> <li>• Large, and</li> <li>• Multi-risk for content harmful to children</li> </ul>                        |
| GA5 | Track unusual increases or new kinds of Primary-Priority Content, Priority Content, and Non-designated Content on the service that may be becoming present on the service | All user-to-user services that are: <ul style="list-style-type: none"> <li>• Large, or</li> <li>• Multi-risk for content harmful to children.</li> </ul> All search services that are: <ul style="list-style-type: none"> <li>• Large general search, or</li> <li>• Multi-risk for content harmful to children</li> </ul>          |
| GA6 | Have a Code of Conduct that sets standards for employees around protecting children   | All user-to-user services that are: <ul style="list-style-type: none"> <li>• Large, or</li> <li>• Multi-risk for content harmful to children.</li> </ul> All search services that are: <ul style="list-style-type: none"> <li>• Large general search services, or</li> <li>• Multi-risk for content harmful to children</li> </ul> |
| GA7 | Ensure staff involved in the design and operational management of service are sufficiently trained in approach to compliance with children’s safety duties                | All user-to-user services that are: <ul style="list-style-type: none"> <li>• Large, or</li> <li>• Multi-risk for content harmful to children.</li> </ul> All search services that are: <ul style="list-style-type: none"> <li>• Large general search services, or</li> <li>• Multi-risk for content harmful to children</li> </ul> |

## Safer platform design choices

We are also proposing a range of safety measures that focus on service providers ensuring they make foundational design choices, so children have safer online experiences. These cover three broad topics:

- **understanding which users are children so that those children can be kept safe;**
- **ensuring recommender systems do not operate to harm children; and**
- **making sure content moderation systems operate effectively.**

## Understanding which users are children so they can be protected online

We do not want children to be denied their rights or enjoying the benefits of being online, but they should be protected from exposure to harmful content.

“I think social media companies need to actually enforce the age limits with an ID check or something [else].” 16-17-year-old<sup>7</sup>

We are proposing broader use of age assurance so that services know which of their users are children, so they have a safe experience online. Where we recommend services use age assurance, we propose that they use what we refer to as ‘highly effective age assurance’.

This is age assurance that is highly effective at correctly determining whether or not a user is a child. We propose that the age assurance used should fulfil the criteria of technical accuracy, robustness, reliability, and fairness. We have published our draft guidance on highly effective age assurance at Annex 10.

Our proposals recognise that age assurance is not a silver bullet and will not be the only effective solution to protect children in all scenarios. We are therefore recommending that highly effective age assurance be used in the areas where it can have the most impact in protecting children online. We have also been mindful of the need to preserve the rights of adult users in accessing legal content.

Ultimately, our proposals are designed to protect children from encountering harmful content, and to strengthen the effectiveness of other measures we set out further below (which might rely on knowing the age of a user).

### Our proposals – in brief

| #   | Proposed measure   | Who should implement this  |
|-----|--|--|
| AA1 | Use highly effective age assurance to prevent children from accessing the entire service   | All user-to-user services whose principal purpose is the hosting or the dissemination of one or more kinds of Primary Priority Content.  |
| AA2 | Use highly effective age assurance to prevent children from accessing the entire service   | All user-to-user services: <ul style="list-style-type: none"><li>• Whose principal purpose is the hosting or the dissemination of one or more kinds of Priority Content, and</li><li>• Who are medium or high risk for one or more of those kinds of Priority Content.</li></ul> |
| AA3 | Use highly effective age assurance to ensure children are prevented from encountering Primary Priority Content identified on the service | All user-to-user services: <ul style="list-style-type: none"><li>• Whose principal purpose is not the hosting or the dissemination of one or more kinds of Primary Priority Content, and</li><li>• Who do not prohibit one or more kinds of Primary Priority Content.</li></ul>  |

<sup>7</sup> Ofcom, 2024. [Children’s Attitudes to Reporting Content Online](#).

| #   | Proposed measure   | Who should implement this  |
|-----|--|--|
| AA4 | Use highly effective age assurance to ensure children are protected from encountering Priority Content identified on the service | All user-to-user services: <ul style="list-style-type: none"> <li>• Whose principal purpose is not the hosting or the dissemination of one or more kinds of Priority Content, and</li> <li>• Who do not prohibit one or more kinds of Priority Content, and</li> <li>• Are medium or high risk for one or more kinds of Priority Content that they do not prohibit.</li> </ul> |
| AA5 | Use highly effective age assurance to apply relevant recommender system measures in the Code to children (see below)             | User-to-user services that: <ul style="list-style-type: none"> <li>• Are medium or high risk for one or more kinds of Primary Priority Content, and</li> <li>• Operate a content recommender system</li> </ul>   |
| AA6 | Use highly effective age assurance to apply relevant recommender system measures in the Code to children (see below)             | User-to-user services that: <ul style="list-style-type: none"> <li>• Are medium or high risk for one or more kinds of relevant Priority Content (excluding bullying), and</li> <li>• Operate a content recommender system</li> </ul>   |

## Ensuring recommender systems do not operate to harm children

Recommender systems are a primary method for sharing users’ content across services. Recommender systems use algorithms to curate and determine how content is shown to users (including children) based on their characteristics, inferred interests, and behaviour. They are generally designed to make the service more appealing to users, by showing them content that the recommender system determines is likely to be of interest to them.

Evidence shows that recommender systems are a key pathway for children to encounter harmful content, including suicide, self-harm and eating disorder content, violent content, and pornographic content. They also play a part in narrowing down the type of content presented to a user, which can lead to increasingly harmful content recommendations as well as exposing users to cumulative harm over time through repeated exposure to harmful content or harmful combinations of content.

“It’s like an algorithm. If you watch [violent content], you get more of it.” – 15 years old<sup>8</sup>

We are therefore proposing three safety measures targeting the design and operation of recommender systems to ensure children are protected from encountering harmful content on recommended feeds and have more control over the content that is recommended to them. We think these will work together to mitigate the risks of harm that recommender systems pose to children, in particular the risk of exposure to cumulative harm.

### Our proposals – in brief

| #   | Proposed measure   | Who should implement this   |
|-----|--|---|
| RS1 | Ensure that content likely to be Primary Priority Content is not recommended to children | All user-to-user services that: <ul style="list-style-type: none"> <li>• Operate a content recommender system, and</li> <li>• Are medium or high risk for at least one kind of Primary Priority Content.</li> </ul> |

<sup>8</sup> Ofcom, 2024. [Understanding Pathways to Online Violent Content Among Children.](#)

| #   | Proposed measure  | Who should implement this  |
|-----|---|--|
| RS2 | Ensure that content likely to be Priority Content is reduced in prominence on children’s recommender feeds <sup>9</sup> | All user-to-user services that: <ul style="list-style-type: none"> <li>• Operate a content recommender system, and</li> <li>• Are medium or high risk for at least one kind of Priority Content (excluding bullying)<sup>10</sup></li> </ul>   |
| RS3 | Enable children to provide negative feedback on content that is recommended to them.                                    | All user-to-user services that: <ul style="list-style-type: none"> <li>• Operate a content recommender system,</li> <li>• Are medium or high risk for at least two kinds of Primary Priority Content and/or Priority Content (excluding bullying)<sup>11</sup>, and</li> <li>• Are large.</li> </ul> |

In our Illegal Harms Consultation, we proposed a safety measure for service providers to collect metrics on recommender systems and use the collected data to assess whether any changes are likely to increase user exposure to illegal content. This previous proposal will also help protect children from illegal content.

### Making sure moderation systems work effectively

Content moderation is the process by which a service reviews content to decide how it should be treated on its service. If it is content harmful to children and access to it should therefore be restricted, services should take steps to ensure children are prevented or protected from encountering it. Content moderation can be done automatically using technology, by human moderators, or a combination of the two. Content moderation plays a hugely important role in keeping users safe from harm – especially children.

Evidence shows that content harmful to children is available on many services at scale, and that children are regularly exposed to it. This suggests that services’ current efforts to protect children from harmful content – including content moderation – are not working well enough.

We are therefore proposing safety measures that target the effectiveness of content moderation systems on user-to-user and search services. They are focused on making sure services have in place effective systems and processes to act on content that is harmful to children, clear policies on what is allowed, adequate moderation resources, and effective systems to prioritise how content is moderated. We think these measures will support more effective content moderation systems and processes, in turn reducing the likelihood that children encounter harmful content.

We ultimately expect all user-to-user and search services to put in place effective systems to address content that is harmful to children and take swift action to protect them from it. This might include

---

<sup>9</sup> We are also minded to extend this measure so that it would apply to certain categories of Non-Designated Content (NDC), namely body image content and depressive content, subject to the outcome of the consultation on NDC. This would mean recommender systems also reducing the prominence of these two types of NDC.

<sup>10</sup> We are proposing not to include risks associated with bullying content due to the limited evidence at this stage of the connection between recommender systems and risks of harm relating to bullying. We are also minded to include two potential kinds of NDC, subject to consultation.

<sup>11</sup> We are also minded to extend this measure for two potential kinds of NDC. Refer to Volume 5, Section 20 for more information.



ensuring such content is not shown to children or taking the content down if it is not permitted. For both large and multi-risk services, we propose a package of more comprehensive measures to ensure that these processes are fit for purpose given the more complex risk environment these services operate in. This set of proposals does not include expectations on the use of automated tools to detect and review content. However, we are aware that large services often do so to handle the scale of content and are exploring how to incorporate measures on automated tools into our Codes.

We have aimed to adopt a consistent approach to our Illegal Harms Consultation for our proposals on content moderation. We therefore think services can take a cohesive approach when considering our proposed codes in the round. We are proposing one additional measure for user-to-user services that use volunteer moderation to mitigate the specific risks they pose to children (see CM7 below). We are also proposing to extend this measure to services at risk of illegal harms (see 4G below).

### Our proposals – in brief

| #                    | Proposed measure  | Who should implement this   |
|----------------------|---|---|
| <b>CM1</b>           | Content moderation systems and processes designed to swiftly take action against content harmful to children  | All user-to-user services   |
| <b>SM1</b>           | Have moderation systems and processes in place to take appropriate action: <ul style="list-style-type: none"> <li>• When Primary Priority Content has been identified, downrank and/or blur the search content</li> <li>• When Priority Content and Non-designated Content has been identified, consider if it is appropriate to downrank and/or blur the search content</li> </ul> | All search services   |
| <b>SM2</b>           | When a user is believed to be a child, filter identified Primary Priority Content out of their search results through a safe search setting. Users believed to be a child should not be able to turn this setting off   | All large general search services   |
| <b>CM2 &amp; SM3</b> | Set and record internal content policies  | All user-to-user services that are: <ul style="list-style-type: none"> <li>• Large, or</li> <li>• Multi-risk for content harmful to children.</li> </ul> All services that are: <ul style="list-style-type: none"> <li>• Large general search services, or</li> <li>• Multi-risk search services</li> </ul> |
| <b>CM3 &amp; SM4</b> | Set performance targets for content moderation function   | All user-to-user services that are: <ul style="list-style-type: none"> <li>• Large, or</li> <li>• Multi-risk for content harmful to children.</li> </ul> All services that are: <ul style="list-style-type: none"> <li>• Large general search services, or</li> <li>• Multi-risk search services</li> </ul> |

| #                    | Proposed measure  | Who should implement this   |
|----------------------|---|---|
| <b>CM4 &amp; SM5</b> | Develop and apply policies on prioritisation of content for review  | All user-to-user services that are: <ul style="list-style-type: none"> <li>• Large, or</li> <li>• Multi-risk for content harmful to children.</li> </ul> All services that are: <ul style="list-style-type: none"> <li>• Large general search services, or</li> <li>• Multi-risk search services</li> </ul> |
| <b>CM5 &amp; SM6</b> | Ensure content moderation functions are well-resourced  | All user-to-user services that are: <ul style="list-style-type: none"> <li>• Large, or</li> <li>• Multi-risk for content harmful to children.</li> </ul> All services that are: <ul style="list-style-type: none"> <li>• Large general search services, or</li> <li>• Multi-risk search services</li> </ul> |
| <b>CM6 &amp; SM7</b> | Ensure content moderation teams are appropriately trained<br><br>Ensure people working in search moderation receive training and materials          | All user-to-user services that are: <ul style="list-style-type: none"> <li>• Large, or</li> <li>• Multi-risk for content harmful to children.</li> </ul> All services that are: <ul style="list-style-type: none"> <li>• Large general search services, or</li> <li>• Multi-risk search services</li> </ul> |
| <b>CM7</b>           | Volunteer moderators should be provided with materials for their roles  | All user-to-user services that use volunteer moderation and are either (or both): <ul style="list-style-type: none"> <li>• Large, or</li> <li>• Multi-risk for content harmful to children.</li> </ul>  |
| <b>4G</b>            | <b>New measure relating to 2023 Illegal Harms Consultation:</b> If volunteer moderation is used, provide moderators with materials for their roles. | All user-to-user services that use volunteer moderation and are either: <ul style="list-style-type: none"> <li>• High/medium risk for at least two kinds of illegal harms</li> <li>• Low risk and large</li> </ul>  |

## Providing children with information, tools, and support

We are also proposing a range of safety measures that focus on service providers providing children with information, tools, and support that will help to keep them safer online. These cover three broad topics:

- having clear terms of service and publicly available statements;
- making sure children can easily report content and make complaints; and
- providing children with tools and support to help them stay safe.

### Having clear terms of service and publicly available statements

Terms of service ('terms') and publicly available statements ('statements') typically lay out the rights and responsibilities that a service provider and the users of their service have towards one another. Terms and statements tend to contain information about how a service functions, including who is allowed to use the service, rules for using the service and how users will be protected from harm on the service.

Children and the adults who care for them need to refer to terms or statements if they want to understand the provisions providers have in place to help protect them. If this information is not provided by a service or if the information is presented in a confusing or inaccessible way, children and carers might not be able to make informed choices about whether to use a service. In addition, it might be difficult for them to know what content is allowed and recognise content that is harmful and report it. This could contribute to the prolonged presence of content harmful to children on a service.

“The rules they show you are paragraphs long and no one reads all that.” 13-15-year-old<sup>12</sup>

We are therefore proposing that all user-to-user and search services should ensure their terms of service and/or publicly available statements are comprehensive, clear, and accessible for children and the adults that care for them. Children should be able to understand what content is allowed on a service and what is not – and this should be presented as clearly as possible.

We think our proposals will increase children’s knowledge and confidence in using online services, including any means the service provides for them to control their own user experience. This in turn should help children to recognise and submit a report or complaint if they are exposed to harmful content online. This should contribute to a safer online environment for children.

Our proposals are broadly consistent with the measures proposed in our Illegal Harms Consultation. However, we are proposing a new measure for providers of Category 1 and 2A services – that they should summarise the findings of their most recent children’s risk assessment in their terms or statement.

We are also proposing an equivalent measure (6AA) for Category 1 and 2A services relating to their illegal content risk assessment to add to the proposals set out in our Illegal Harms Consultation. This measure recommends that Category 1 and 2A services should summarise the findings of their most recent illegal content risk assessment in their terms or statement so that it is clear what risks and potential harms individuals could experience on the service.

### Our proposals – in brief

| #   | Proposed measure   | Who should implement this                           |
|-----|--|---|
| TS1 | Terms and statements regarding the protection of children should contain all information mandated by the Act   | All user-to-user services<br>All search services    |
| TS2 | Terms and statements regarding the protection of children should be clear and accessible   | All user-to-user services<br>All search services    |
| TS3 | Services should summarise the findings of their most recent children’s risk assessment in their terms or statements  | All Category 1 services<br>All Category 2A services |
| 6AA | <b>New measure relating to 2023 Illegal Harms Consultation:</b> Services should summarise the findings of their most recent illegal content risk assessment in their terms or statements | All Category 1 services<br>All Category 2A services |

<sup>12</sup> Ofcom, 2024. [Children’s Attitudes to Reporting Content Online.](#)

## Making sure children can easily report content and make complaints

User reporting and complaints allow users – including children – to make service providers aware of when harmful content is present on their service, or when content has been mistakenly removed or restricted. They both play an important role in protecting children online and protecting users’ rights.

While many services already have reporting and complaints functions available to users, our evidence suggests that children do not think these are always accessible, easy to use and transparent. This can discourage people from using these functions, including children.

“I think the report button should always be highlighted... to make it stand out and easy to find.”  
13-15-year-old<sup>13</sup>

In our Illegal Harms Consultation, we suggested several measures focused on improving how service providers handle complaints and reports to help them comply with the Act. In this consultation, we are proposing additional measures to drive further improvements and ensure services meet their responsibilities effectively. These new measures require services likely to be accessed by children to offer clear, straightforward, and accessible complaints procedures. They must also respond to complaints promptly and take suitable action.

Our proposed measures refer to ‘complaints’, which include user reports, appeals and other types of complaints, such as complaints about a service not complying with its duties to protect children. User reports are a specific type of complaint about content, submitted through a reporting tool. Appeals are complaints by users who believe a service has made an incorrect decision about a piece of content.

We know that many providers operate a single complaints process for various types of complaints. We have taken this into account when assessing what measures to propose in the Children’s Safety Codes. Many of the proposed measures align with measures in the draft Illegal Content Codes. Measures UR2 and UR3 below include additional elements, which we provisionally think should be included in both the Children’s Safety Codes and the Illegal Content Codes. These are recommendations that services should explain to complainants when they make a complaint what, if any, information they will provide, and services should include information about the resolution of complaints in the acknowledgement they send to complainants.

We are proposing to expand these measures due to new evidence showing that children are worried about the confidentiality of complaint processes and that poor communication from services about complaints can undermine trust in the entire process. Consequently, we suggest that services should improve how they explain their complaint procedures to users, aiming to make these mechanisms more transparent.

We believe these measures will ensure services have effective complaints procedures in place, which will help them take steps to protect children from encountering harmful content and improve any systems they use to detect harmful content. This will ensure services can be made safer for children, accountable and respectful of user rights.

---

<sup>13</sup> Ofcom, [Children’s Attitudes to Reporting Content Online](#), 2024

## Our proposals – in brief

| #   | Proposed measure  | Who should implement this                        |
|-----|---|--|
| UR1 | Have complaints processes which enable users to make relevant complaints for services likely to be accessed by children       | All user-to-user services<br>All search services |
| UR2 | Have easy to access and use, and transparent complaints systems   | All user-to-user services<br>All search services |
| UR3 | Acknowledge receipt of complaints with indicative timeframe and information on resolution                                     | All user-to-user services<br>All search services |
| UR4 | User-to-user services take appropriate action in response to each complaint   | All user-to-user services                        |
| UR5 | Search services take appropriate action in response to each complaint   | All search services                              |
| SD1 | Offer users a way of easily reporting predictive search suggestions relating to primary priority content and priority content | All large general search services                |

## Providing children with tools and support to stay safe

Many services have functionalities that allow users to connect with one another, such as group messaging or comment sections. These functionalities can pose risks to children, as they can allow users to expose children to harmful content or activity without their consent.

“I think they could have tighter [restrictions on] who can contact who, because then it could avoid ... people getting added to things like group chats...” 14-17-year-old<sup>14</sup>

We have proposed user support measures which we believe will give children more control over their online experience and help them stay safe online. For user-to-user services, we are proposing:

- **user support tools** that will enable children to have more control over their interactions on services that pose a risk of harm, by giving them the option to decline group invites, block and mute user accounts, or disable comments on their own posts; and
- **user support materials** for children to both assist their understanding of how they can restrict certain types of online interactions that may put them at risk of harm and to support them when they report, post, or search for certain types of harmful content. These measures apply depending on a service’s risk level and size.

These measures broadly mirror those that we proposed relating to user support in our Illegal Harms Consultation. Measure US4 is also an adapted version of a measure in our Illegal Harms Consultation – we are proposing for certain types of services to provide information to child users when they restrict interactions with other accounts or content. We will consider whether to apply this additional element to our Illegal Harms Codes ahead of finalising them. We are also proposing three user support measures for the Children’s Safety Codes that do not have an equivalent in our proposed Illegal Harms Codes.

<sup>14</sup> Ofcom, 2024. [Key attributes and experiences of cyberbullying among children in the UK.](#)

For search services, we are also proposing a measure to provide crisis prevention information in response to search requests for known primary priority content (which includes self-harm and suicide content). Crisis prevention information includes help and support such as helplines and supportive information from reputable organisations. This measure is also consistent with what we proposed in our Illegal Harms Consultation.

We believe these measures will give children more control over their online interactions and provide added support while online to help keep them safe.

### Our proposals – in brief

| #   | Proposed measure   | Who should implement this  |
|-----|--|--|
| US1 | Provide children with an option to accept or decline an invite to a group chat                             | All user-to-user services that: <ul style="list-style-type: none"> <li>• Have group chats, and</li> <li>• Are medium or high risk of one or more of: pornographic content, eating disorder content, bullying content, abuse and hate content<sup>15</sup> and violent content.<sup>16</sup></li> </ul> |
| US2 | Provide children with the option to block and mute other users' accounts                                   | All user-to-user services that: <ul style="list-style-type: none"> <li>• Have user profiles and certain user interaction functionalities,<sup>17</sup> and</li> <li>• Are medium or high risk of one of more of: bullying content, abuse and hate content and violent content</li> </ul>               |
| US3 | Provide children with the option to disable comments on their own posts                                    | All user-to-user services that: <ul style="list-style-type: none"> <li>• Have comment functionalities, and</li> <li>• Are medium or high risk of one or more of: bullying content, abuse and hate content and violent content</li> </ul>   |
| US4 | The provision of information to child users when they restrict interactions with other accounts or content | All user-to-user services that: <ul style="list-style-type: none"> <li>• Have certain functionalities that restrict interactions with other accounts or content,<sup>18</sup> and</li> <li>• Are large, and</li> <li>• Are multi-risk for content harmful to children</li> </ul>                       |
| US5 | Signpost children to support at key points in the user journey   | Intervention point 1 – when children report content<br>All user-to-user services that <ul style="list-style-type: none"> <li>• Are medium or high risk of one or more of: suicide content, self-harm content,</li> </ul>   |

<sup>15</sup> We use 'abuse and hate' content to refer to the two kinds of content defined in the Act in sections 62(2) and 62(3). A service is considered to have medium or high risk for abuse and hate content if it has medium or high risk for at least one of the two kinds of content defined in the Act in sections 62(2) and 62(3).

<sup>16</sup> We use 'violent content' to refer to the three kinds of content defined in the Act in sections 62(4), 62(6) and 62(7). A service is considered to have medium or high risk for violent content if it has medium or high risk for at least one of the three kinds of content defined in the Act in sections 62(4), 62(6) and 62(7).

<sup>17</sup> These functionalities include user connections, posting content, and user communication. For more information, please refer to Volume 5, Section 20.

<sup>18</sup> Please refer to Volume 5, Section 20 for more information on the functionalities that are applicable to Measure US4.

|            |   |   |
|------------|---|---|
|            |   | <p>eating disorder content, or bullying content</p> <p>Intervention point 2 – when children post or re-post content</p> <p>Large user-to-user services that</p> <ul style="list-style-type: none"> <li>• Have posting/re-posting functionalities, and</li> <li>• Are medium or high risk of one or more of: suicide content, self-harm content, eating disorder content, or bullying content, and</li> <li>• Have measures that enable them to identify when a user posts or re-posts suicide, self-harm, eating disorder or bullying content</li> </ul> <p>Intervention point 3 – when children search for harmful content:</p> <p>All user-to-user services that</p> <ul style="list-style-type: none"> <li>• Have user-generated content searching, and</li> <li>• Are high or medium risk of one or more of: suicide content, self-harm content, eating disorder content, and</li> <li>• Have measures that enable them to become aware of when a user searches using suicide, self-harm or eating disorder related search terms</li> </ul> |
| <b>US6</b> | Provide age-appropriate user support materials for children   | <p>All user-to-user services that are multi-risk for content harmful to children</p> <p>All search services that are multi-risk for content harmful to children</p>   |
| <b>SD2</b> | Provide crisis prevention information in response to known Primary Priority Content-search requests regarding suicide, self-harm and eating disorders | All large general search services   |

## How we determine which services should implement each measure

The Act requires us to take into account several principles in developing our proposals. We must ensure that the measures set out in our Codes are compatible with the online safety objectives set out in the Act, which includes that services should be designed and operated in a way that provides a higher standard of protection for children than adults. Therefore, developing a set of measures that ensures services have the systems and processes in place to reduce risks to children has been central to our approach. This has allowed us to identify which measures are most effective at protecting children and to target those measures towards services where children face the greatest risks.

At the same time, the Act is clear that in designing Codes we should ensure that any proposals are proportionate to the risk of harm presented by services of that kind and size. We recognise that the size, capacity, functionalities, user base and risks of online services in scope of the children's safety duties differ widely. For this reason, we have not taken a one-size-fits-all approach and proposed different measures according to the level of risk posed by services, their size, and resources.

This does not mean that smaller risky services can fail to fulfil their duties to keep children safe because they have fewer resources. Instead, we consider the regulatory burden of our measures on services to ensure that protecting children online does not unduly undermine innovation and investment in high-quality online services that all UK users can enjoy.

As a result, we propose that all services accessed by children – regardless of their size or risk – implement a core set of measures to protect children online. We propose additional measures for services that pose a greater risk of harm to children, recommending costly measures for smaller services only where there is clear risk of harm and where we have evidence that the measures proposed will make a material difference in dealing with this risk. Larger and better-resourced services that pose the most material risks to many children will be expected to go even further.

This means in practice that each measure is ultimately recommended based on relevant criteria, which include:

- **the type of service**, including distinguishing between user-or-user and search services where appropriate;
- **the outcome of the service's latest risk assessment**, and what risks have been identified in relation to content harmful to children; and
- **relevant functionalities and other characteristics** of a service that have been shown to pose risks to children; and
- **the size of a service**, in terms of its UK user base. Where we refer to the size of the service provider, we have proposed the following definitions:
  - **large services**: we propose to define a service as 'large' where it has an average user base greater than seven million per month in the UK, approximately equivalent to 10% of the UK population; and
  - **smaller services**: these are all services that do not fall into the 'large' category.



# What we have published

This consultation includes five volumes which set out our analysis and the approach we have taken, plus the draft versions of the codes and guidance we are required to produce. We provide an overview below for ease of reference.

## **Volume 1: Overview, scope and regulatory approach**

Volume 1 provides an overview of the consultation. We also explain the scope of our consultation and the legal basis of our proposals, including what we mean by content harmful to children, and how our proposals fit into Ofcom's overall strategy for online safety.

## **Volume 2: Identifying the services children are using**

Volume 2 explains how we have approached our draft Children's Access Assessments Guidance. This is the process all service providers must go through to assess whether a service is likely to be accessed by children. Our draft [Children's Access Assessments Guidance](#) is published separately. We have also published our related [draft guidance on what constitutes highly effective age assurance](#).

## **Volume 3: The causes and impacts of harm to children**

Volume 3 presents our assessment of how content harmful to children manifests online, what factors cause risks of harm, and the impact of harmful content on children. Our analysis in this volume incorporates two regulatory products – our draft Children's Register of Risks, and our draft Guidance on Content Harmful to Children.

## **Volume 4: Assessing the risks of harms to children online**

Volume 4 sets out our proposed approach to how service providers should assess the risks their service(s) pose to children. We set out our proposed approach to the guidance we are required to produce for services about children's risk assessments, and our proposals for how services should approach governance and accountability in relation to the children's safety duties in the Act. Our draft [Children's Risk Assessment Guidance](#) is published separately.

## **Volume 5: What should services do to mitigate the risk of online harms to children?**

Volume 5 explains the measures we propose services take to keep children safe online. These measures form our draft Children's Safety Codes, which are published separately for [user-to-user services](#) and for [search services](#). We have also published our draft guidance on highly effective age assurance.