

Protecting children from harms online

Annexes 1-4

Consultation

Published 8 May 2024

Closing date for responses: 17 July 2024

Contents

Annex

A1. Responding to this consultation	3
A2. Ofcom’s consultation principles	5
A3. Consultation coversheet.....	6
A4. Consultation questions	9

A1. Responding to this consultation

How to respond

- A1.1 Ofcom would like to receive views and comments on the issues raised in this consultation, by 5pm on 17 July 2024
- A1.2 You can download a response form from <https://www.ofcom.org.uk/consultations-and-statements/category-1/protecting-children-from-harms-online>. You can return this by email or post to the address provided in the response form.
- A1.3 If your response is a large file, or has supporting charts, tables or other data, please email it to protectingchildren@ofcom.org.uk, as an attachment in Microsoft Word format, together with the cover sheet. This email address is for this consultation only and will not be valid after 17 July 2024.
- A1.4 Responses may alternatively be posted to the address below, marked with the title of the consultation.
- Ofcom Online Safety Team
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA
- A1.5 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:
- send us a recording of you signing your response. This should be no longer than 5 minutes. Suitable file formats are DVDs, wmv or QuickTime files; or
 - upload a video of you signing your response directly to YouTube (or another hosting site) and send us the link.
- A1.6 We will publish a transcript of any audio or video responses we receive (unless your response is confidential)
- A1.7 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt of a response submitted to us by email.
- A1.8 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt of a response submitted to us by email.
- A1.9 It would be helpful if your response could include direct answers to the questions asked in the consultation document. The questions are listed at Annex 4. It would also help if you could explain why you hold your views, and what you think the effect of Ofcom's proposals would be.
- A1.10 If you want to discuss the issues and questions raised in this consultation, please email to protectingchildren@ofcom.org.uk

Confidentiality

- A1.11 Consultations are more effective if we publish the responses before the consultation period closes. This can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish responses on the Ofcom website at regular intervals during and after the consultation period.
- A1.12 If you think your response should be kept confidential, please specify which part(s) this applies to and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.
- A1.13 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it, either by not publishing the response at all, or by only publishing the bits that are not confidential. Sometimes we might think it is important to disclose parts of a response that have been marked as confidential for reasons of transparency, but we will consult you before we do. Occasionally we might have a legal obligation to publish information or disclose it in court, but again, as far as possible, we will let you know.
- A1.14 Even if your response is not marked as confidential, we might still decide not to publish all or part of it in certain circumstances. For example, if we have concerns about the impact on your privacy or the privacy of others, that the content of the response might facilitate the commission of crime, or about the sensitive nature of the content more generally. If we decide not to publish all or part of your response, we will still take it into account in our consideration of the matter.
- A1.15 To fulfil our pre-disclosure duty, we may share a copy of your response with the relevant government department before we publish it on our website.
- A1.16 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our Terms of Use.

Next steps

- A1.17 Following this consultation period, Ofcom plans to publish a statement in spring 2025.
- A1.18 If you wish, you can register to receive email updates alerting you to new Ofcom publications.

Ofcom's consultation processes

- A1.19 Ofcom aims to make responding to a consultation as easy as possible. For more information, please see our consultation principles in Annex 2.
- A1.20 If you have any comments or suggestions on how we manage our consultations, please email us at consult@ofcom.org.uk. We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and individual users, who are less likely to give their opinions through a formal consultation.

A1.21 If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact the corporation secretary:

A1.22 Corporation Secretary

Ofcom

Riverside House

2a Southwark Bridge Road

London SE1 9HA

Email: corporationsecretary@ofcom.org.uk

DRAFT

A2. Ofcom's consultation principles

Ofcom has seven principles that it follows for every public written consultation:

Before the consultation

- A2.1 Wherever possible, we will hold informal talks with people and organisations before announcing a big consultation, to find out whether we are thinking along the right lines. If we do not have enough time to do this, we will hold an open meeting to explain our proposals, shortly after announcing the consultation.

During the consultation

- A2.2 We will be clear about whom we are consulting, why, on what questions and for how long.
- A2.3 We will make the consultation document as short and simple as possible, with an overview of no more than two pages. We will try to make it as easy as possible for people to give us a written response.
- A2.4 When setting the length of the consultation period, we will consider the nature of our proposals and their potential impact. We will always make clear the closing date for responses.
- A2.5 A person within Ofcom will be in charge of making sure we follow our own guidelines and aim to reach the largest possible number of people and organisations who may be interested in the outcome of our decisions. Ofcom's Consultation Champion is the main person to contact if you have views on the way we run our consultations.
- A2.6 If we are not able to follow any of these seven principles, we will explain why.

After the consultation

- A2.7 We think it is important that everyone who is interested in an issue can see other people's views, so we usually publish the responses on our website at regular intervals during and after the consultation period. After the consultation we will make our decisions and publish a statement explaining what we are going to do, and why, showing how respondents' views helped to shape these decisions.

A3. Consultation coversheet

Basic details

Consultation title: OSA Children's Consultation

To (Ofcom contact):

Name of respondent:

Representing: Epic Games

Address (if not received by email):

Confidentiality

Please tick below what part of your response you consider is confidential, giving your reasons why

- > Nothing
- > Name/contact details/job title
- > Whole response
- > Organisation
- > Part of the response

If you selected 'Part of the response', please specify which parts:

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

Yes No

Declaration

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom aims to publish responses at regular intervals during and after the consultation period. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name

Signed (if hard copy)

A4. Consultation questions

We welcome views and evidence on the questions below. It is not necessary to answer every question – please answer those on which you have a view.

Respondents do not need to repeat comments they have made in response to our Illegal Harms Consultation when responding to this consultation. If you have already responded to the Illegal Harms Consultation and would like us to consider some or all of your response in relation to this consultation, please let us know.

Volume 2: Identifying the services children are using

Children's Access Assessments (Section 4)

Do you agree with our proposals in relation to children's access assessments, in particular the aspects below. Please provide evidence to support your view.

1. Our proposal that service providers should only conclude that children are not normally able to access a service where they are using highly effective age assurance?
2. Our proposed approach to the child user condition, including our proposed interpretation of "significant number of users who are children" and the factors that service providers consider in assessing whether the child user condition is met?
3. Our proposed approach to the process for children's access assessments?

Volume 3: The causes and impacts of online harm to children

Draft Children's Register of Risk (Section 7)

Proposed approach

4. Do you have any views on Ofcom's assessment of the causes and impacts of online harms? Please provide evidence to support your answer.
 - a. Do you think we have missed anything important in our analysis?
5. Do you have any views about our interpretation of the links between risk factors and different kinds of content harmful to children? Please provide evidence to support your answer.
6. Do you have any views on the age groups we recommended for assessing risk by age? Please provide evidence to support your answer.
7. Do you have any views on our interpretation of non-designated content or our approach to identifying non-designated content? Please provide evidence to support your answer.

Evidence gathering for future work

8. Do you have any evidence relating to kinds of content that increase the risk of harm from Primary Priority, Priority or Non-designated Content, when viewed in combination (to be considered as part of cumulative harm)?
9. Have you identified risks to children from GenAI content or applications on U2U or Search services?
 - a. Please Provide any information about any risks identified
10. Do you have any specific evidence relevant to our assessment of body image content and depressive content as kinds of non-designated content? Specifically, we are interested in:
 - a. (i) specific examples of body image or depressive content linked to significant harms to children,
 - b. (ii) evidence distinguishing body image or depressive content from existing categories of priority or primary priority content.
11. Do you propose any other category of content that could meet the definition of NDC under the Act at this stage? Please provide evidence to support your answer.

Draft Guidance on Content Harmful to Children (Section 8)

12. Do you agree with our proposed approach, including the level of specificity of examples given and the proposal to include contextual information for services to consider?
13. Do you have further evidence that can support the guidance provided on different kinds of content harmful to children?
14. For each of the harms discussed, are there additional categories of content that Ofcom
 - a. should consider to be harmful or
 - b. consider not to be harmful or where our current proposals should be reconsidered

Volume 4: How should services assess the risk of online harms?

Governance and Accountability (Section 11)

15. Do you agree with the proposed governance measures to be included in the Children's Safety Codes?
 - a. Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence.
 - b. If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response.
16. Do you agree with our assumption that the proposed governance measures for Children's Safety Codes could be implemented through the same process as the equivalent draft Illegal Content Codes?

Children’s Risk Assessment Guidance and Children’s Risk Profiles’ (Section 12)

17. What do you think about our proposals in relation to the Children’s Risk Assessment Guidance?
- Please provide underlying arguments and evidence of efficacy or risks that support your view.

Comments on consultation

Updating risk assessments

Similar to what was set out in the Illegal Harms Consultation, Ofcom has said that for “a significant change to the service” it may still require businesses to “carry out a new children’s risk assessment relating to the change” (section 12.93).

However, the ‘significant changes’ that Ofcom describes are part of the day-to-day pace of how gaming services operate and innovate. Requiring services to carry out entirely new risk assessments before making the kinds of changes described in the consultation, in addition to the annual risk assessment, is challenging – services would be in a constant state of creating new risk assessments, which would likely be out of date quickly when a new policy or feature launches. Ofcom could consider making the risk assessment process lighter and less resource-intensive, or changing the requirement so that services need only update relevant portions of their existing risk assessment, rather than having to carry out a new one.

18. What do you think about our proposals in relation to the Children’s Risk Profiles for Content Harmful to Children?
- Please provide underlying arguments and evidence of efficacy or risks that support your view.

Specifically, we welcome evidence from regulated services on the following:

19. Do you think the four-step risk assessment process and the Children’s Risk Profiles are useful models to help services understand the risks that their services pose to children and comply with their child risk assessment obligations under the Act?
20. Are there any specific aspects of the children’s risk assessment duties that you consider need additional guidance beyond what we have proposed in our draft?
21. Are the Children’s Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service?
- If you have comments or input related to the links between different kinds of content harmful to children and risk factors, please refer to Volume 3: Causes and Impacts of Harms to Children Online which includes the draft Children’s Register of Risks.

Volume 5 – What should services do to mitigate the risk of online harms

Our proposals for the Children’s Safety Codes (Section 13)

Proposed measures

22. Do you agree with our proposed package of measures for the first Children’s Safety Codes?
- If not, please explain why.

Evidence gathering for future work.

23. Do you currently employ measures or have additional evidence in the areas we have set out for future consideration?
- If so, please provide evidence of the impact, effectiveness and cost of such measures, including any results from trialling or testing of measures.

Comments on consultation

Introduction

Epic Games is a leading interactive entertainment company and provider of 3D engine technology. Headquartered in Cary, North Carolina in the United States, Epic has offices worldwide, including in the United Kingdom. Epic is the creator of Fortnite, a vibrant ecosystem of online entertainment experiences including first-party games like Fortnite Battle Royale, LEGO Fortnite, Rocket Racing, and Fortnite Festival, as well as creator-made experiences. In addition to Fortnite, Epic operates popular games like Rocket League and Fall Guys. Epic also develops the Unreal Engine, which powers many of the world’s leading games and is also adopted across industries such as film and television, architecture, automotive, manufacturing, and simulation. Through the Unreal Engine and Epic Games Store, as well as Epic Online Services, a set of platform-agnostic and free services for game developers to launch, operate and scale their games, Epic provides an end-to-end digital ecosystem for developers and creators to build, distribute, and operate games and other content.

Fortnite has continued to develop beyond the popular Battle Royale game. Players who log into Fortnite today can choose among thousands of games and experiences. These include games created by Epic, such as LEGO Fortnite, Rocket Racing, and Fortnite Festival, as well as games built by smaller and independent developers and individual creators. Epic wants Fortnite to be a welcoming, safe, and fun experience for players of all ages.

Epic’s Approach to Online Safety

Every day millions of players across the Epic Games ecosystem come together to play games and have fun with friends and family. To help keep our spaces welcoming, entertaining, and safe for all players, we set clear guidelines for respectful behavior and provide tools for players and parents to manage their experience.

Epic takes a multi-pronged approach to online safety that starts by providing strong protections for children. By balancing safety and privacy, Epic aims to promote an engaging and age appropriate environment for all users:

- Safety by Design:** High default safety and privacy settings help to keep players under 18 safe, while measures such as Epic’s “Cabined Accounts”¹ provide even more protections for younger players.

- **Parental Controls:** Epic provides parents and guardians with a set of granular controls so they can tailor the experience to one that's right for their family.
- **Moderation:** Epic moderates player conduct and user-generated content, including Fortnite islands, according to its robust Community Rules and Content Guidelines.
- **Age Ratings:** Epic partners with age rating authorities around the world to provide parents and players trusted and familiar age rating information for experiences in our ecosystem. These ratings help parents and players make informed decisions about the games they play across Fortnite and the Epic Games Store, and allow parents to configure parental controls to limit what content their child is allowed to play or purchase.
- **Purchasing Protections:** Epic's games can be played for free, with no pay-to-win mechanics or paid random item loot boxes. The Item Shops in Epic's games are designed to help users understand what to expect when making purchases, and make it easy to cancel unwanted purchases and request refunds.

As Epic's products have evolved, the company has introduced a number of new and innovative safety measures, including Cabined Accounts, Voice Reporting, and age ratings inside Fortnite. These measures are set out in greater detail below.

Cabined Accounts

In December 2022, Epic introduced [Cabined Accounts](#), a new type of Epic account designed to create a safe and inclusive space for younger players. Players with Cabined Accounts can still play Epic games, such as Fortnite, Rocket League and Fall Guys, but won't be able to access certain features such as voice chat until their parent or guardian provides consent.

When a player goes to create an Epic Games account, they are first required to provide their age. If they indicate that they are under 13 or their country's age of digital consent, whichever is higher, their account will be a Cabined Account and they will be asked to provide a parent or guardian's email address to receive consent to access certain features in Epic's products. In the UK, players who indicate that they are under 13 will be placed in a Cabined Account. Parents of players with Cabined Accounts will receive an email from Epic to inform them that their child has created an account with details on how to provide consent for additional features and set up Parental Controls. Parents who provide consent are verified via Epic's [Kids Web Services](#) (KWS).

The following features are disabled in a Cabined Account:

- Communicating with other players using voice chat or free text chat
- Purchasing items with money
- Downloading games that are not owned by Epic
- Recommendations based on past activity
- Email marketing or push notifications
- Sign in with Epic, including linking accounts to certain external services, such as social media websites or video streaming applications
- Custom display names
- SMS-based two-factor authentication

Verifiable Parental Consent

Epic makes it simple for parents and guardians to manage their family's online experience through [Kids Web Services](#) ("KWS"). Kids Web Services enables other developers to manage youth audiences by providing tools for consent management and parent verification, making the process and experience simpler for parents.

KWS is used to obtain verifiable parental consent (“VPC”) before allowing children to access features that require it. Once parents verify that they are an adult, they are added to KWS' ParentGraph, a network of pre-verified parents built on the principle of data minimisation. The service enables verified parents to manage consent for their child in various digital experiences without re-submitting parents' personal data for age verification in every app, game or website their child uses.

KWS aims to empower developers and make online experiences safer for kids by simplifying the verification process for both developers and parents. It is offered to developers for free, at any scale, eliminating all parent verification costs for both developers and parents or guardians. These services are currently used by a number of large account systems, including 2K, LEGO, Niantic, Innersloth, Bandai Namco, and many others.

ParentGraph process:

1. Once a parent email has been gathered by a developer (and the parent has been provided with appropriate notice of the developer's data collection practices), their email address is passed to KWS.
2. KWS invites the parent to select from a choice of verification methods:
 - a. Face scan: Parents in the UK can verify they are an adult using face scan. KWS prompts the parent to hold their device in front of their face. Via the device's camera, a machine-learning algorithm estimates the parent's age. Face scan verification is provided by [Yoti](#).
 - b. ID scan: Parents in the UK can verify they are an adult by scanning the back and front of their ID card or document. This method supports hundreds of types of ID from different jurisdictions; for example, passports, driving licenses, and national ID cards. The scanned ID is verified by [Veriff](#).
 - c. Payment card: Parents in the UK can verify they are an adult using a payment (credit or debit) card. The payment card details are verified by [Stripe](#).
3. KWS verifies they are an adult, and then discards any verification details (e.g. credit card details) collected in the process. Finally, the parent is sent an email confirming their successful verification.
4. At this point, the parent's email address is encrypted using a one-way hash function, which is stored, along with the method and the timestamp of verification, the country in which the parent's device is located, and the app or service in connection with which the parent verified their identity. The verification details provided by the parent (e.g. credit card details) are not stored.
5. The next time the parent's email address is provided to KWS from a new app or platform, KWS again encrypts it using the same hash function, and checks if that hash is already present in the ParentGraph. If it is not, the parent is prompted to go through the normal verification process (as above). If the hash has a match, we know the parent has previously verified their age with KWS and therefore does not need to do so again. In either case, the parent is sent an email confirming their successful verification (and including information about the ParentGraph and an opportunity to opt out of it).

The ParentGraph enables re-use of verification status across multiple services by storing the hashed email address of a verified adult, such that it can only be matched to the same email address encrypted with the same hash function.

The ParentGraph currently contains nearly 24 million verified parents. As the number of verified parents in the ParentGraph grows, more kids will safely get access to the content they want with less friction, fewer parents will be frustrated with the amount of personal data and time that is taken from them, and Parent Verification conversion rates will be continually improved across all types of digital platforms and experiences.

We note that volume 5 contains some useful summaries about different types of HEAA (e.g. age estimation, age verification). However, it would be useful to know if Ofcom is planning to provide any additional clarity or detail regarding what it would consider to be 'highly effective age assurance', since there are of course many third-party providers that have a wide variety of age assurance offerings.

In particular, it would be useful to know if Ofcom is proposing to follow the ICO's approach and adopt the [Age Check Certification Scheme](#).

Default settings for players under 18

As highlighted by the ICO in standard 7 of the Age-Appropriate Design Code, "*many children will just accept whatever default settings you provide*". Having protective default settings for children is therefore a powerful tool for their protection.

Epic has set high default safety and privacy settings for all players under 18 on Fortnite.

- a. Voice chat, text chat, and personalised recommendations are set to "Off" by default for all players under 18.
- b. Player Parties are set to "Private" by default for players under 18, meaning no one can join their party without an invite from them.
- c. The Mature Language Filter is set to "On" by default for all players under 16.
- d. The Parental Controls PIN is required to add new friends by default for players under 10. .

Parental Controls

Epic's Parental Controls let parents and guardians choose how their child plays and interacts with others across Epic's games and experiences, including Fortnite, Rocket League, and Fall Guys. These tools let parents and guardians make informed decisions about what is right for their family and manage access to social features such as voice and text chat, purchasing permissions, and more.

- **Epic Voice and Text Chat Permissions:** Manage who your child is able to speak with using Epic voice chat and text chat.
 - Parents and guardians can allow their child to speak with "Everybody," "Friends & Teammates," "Friends Only," or turn text or voice chat off entirely by selecting "Nobody."
 - If a child is under 10 years old, the maximum voice and text chat permission that parents and guardians can enable in Parental Controls is "Friends Only." And if a child is under 13, the maximum voice and text chat permission is "Friends & Teammates."
- **Filter Mature Language on Fortnite:** Filter out mature language such as profanity in Fortnite's text chat.
- **Require a PIN to Add Friends:** Choose to require your Parental Controls PIN to be entered for your child to send or accept Epic friend requests.
- **Require a PIN for Epic Games Payments:** Choose to require your Parental Controls PIN to be entered to authorise real money purchases using Epic payment.
- **Fortnite Content Ratings:** Every experience in Fortnite has its own rating and you can choose to limit your child's access to experiences above a certain rating. Your Parental Controls PIN will be required to unlock experiences for your child that are rated above your age-rating setting.
- **Allow Creative Mode and Unreal Editor for Fortnite:** Players can use Fortnite Creative and Unreal Editor for Fortnite (UEFN) to design and create experiences in Fortnite. You can choose to restrict your child's access to these toolsets.
- **Epic Games Store Rating:** You can choose the maximum rating for new games your child can buy or download from the Epic Games Store. If your child tries to view, buy, or download a new game above your chosen rating, your Parental Controls PIN will be required.

- **Enable Sign in With Epic for your child:** You can choose to require parental consent for each non-Epic game or site to which your child attempts to log in or connect using their Epic Account, or enable the 'Sign in with Epic' single sign on solution (SSO). Players can use Sign In With Epic to access games or connect to platforms that aren't operated by Epic. When using Sign In With Epic, players share account information including their Epic ID and Display Name, connected gaming account names, their online presence, and their Epic friends list.
- **Fortnite Playtime Tracking Report:** Sign up for weekly playtime reports on the amount of time your child plays Fortnite.
- **Activity Reports for Your Child's Epic Account:** Sign up to receive activity reports when changes are made to your child's Epic account:
 - *Parental Control Settings Updates* - Notifications when your Parental Control PIN is used to make changes to Parental Controls settings on your child's account.
 - *Friend Requests* - Notifications when your Parental Control PIN is used to send or accept a friend request.
 - *New Epic Friends Added* - Notifications of friends added to your child's Epic Friends list.

Moderation

Epic has [Community Rules](#) that apply to all users of Epic's games, services, and environments. Additionally our [Content Guidelines](#) outline content that is prohibited across Epic's experiences, services, and marketplaces.

Consequences for violating Epic's rules and guidelines vary depending on the severity and number of offenses, including the following actions:

- A warning that additional abuses may result in account restrictions.
- Removal of the content that violates our rules.
- A temporary restriction on using certain products, making purchases, adding new friends, or social features like voice or text chat for a specific period of time, depending on the nature of the abuse.
- A permanent account ban that restricts someone from using Epic products.

Players can also block or mute players they no longer wish to interact with. If players suspect that content they encounter in any of Epic's products or services is illegal or violates the company's Community Rules or Content Guidelines, they can use the in-game report function or submit a report using [this form](#).

Epic takes reports of potentially violative content seriously, and uses a combination of automated tools and human moderators to identify and flag content that potentially violates Epic's Community Rules and Content Guidelines. A team of specially-trained moderators reviews flagged reports to determine the appropriate action.

Players can access Epic's [Sanctions & Appeals portal](#) to view sanctions applied to their account and submit appeals. The portal also enables players to see the status and outcome of each of their appeals.

Voice Reporting

In November 2023, Epic launched Voice Reporting in Fortnite. In addition to being able to block, mute and report other players, players are able to submit audio evidence when they report suspected violations of Epic's [Community Rules](#). This helps Epic take action against players using voice chat to bully, harass, discriminate or engage in other inappropriate behavior.

When Voice Reporting is on, the last five minutes of voice chat audio are captured on a rolling basis. This means only the immediate last five minutes of audio is reportable. As new audio is captured, any

previous audio that's more than five minutes old is automatically deleted. Voice chat audio is securely captured on the player's own device (such as a gaming console or PC), not the Epic Games servers. When players report a conversation, the voice chat audio captured from the last five minutes will be uploaded with it and reviewed. Epic has no way of accessing any voice chat audio unless Voice Reporting is on and a participant submits a voice report.

Voice Reporting is always on for voice chats that include players under 18. Players 18 and over can set their Voice Reporting preferences to "Always On" or "Off When Possible." After selecting "Always On," Voice Reporting will be on in every channel that player is in. After selecting "Off When Possible," Voice Reporting will be off in parties formed among friends where all players have voice reporting set to "Off When Possible." Voice Reporting will always be on in all Game Channels, which are channels that connect players on the same team but in different parties.

Age Ratings

In October 2023, Epic announced that in partnership with the [International Age Rating Coalition \(IARC\)](#), Fortnite would begin featuring internationally-recognised age and content ratings for all first and third party playable content. Since November 2023, all experiences published in Fortnite are required to have an IARC-assigned rating ranging from a PEGI 3 to a maximum rating of PEGI 12, giving parents and players access to trusted and familiar ratings that help them make informed decisions about what they play.

When a creator is ready to publish their island to Fortnite, they will fill out the IARC content rating questionnaire before they submit their island for review by Epic moderators. After completing the IARC questionnaire, creators automatically receive region-specific ratings from [IARC-participating rating authorities](#), along with a global age rating for non-participating regions. These ratings are automatically applied and prominently displayed before a player accesses any content in Fortnite. Content sensitivities vary by region and IARC's scalable, global solution provides parents and players with trusted guidance from PEGI (UK and Europe), ACB (Australia), ESRB (North America), USK (Germany), ClassInd (Brazil), GRAC (South Korea) and more depending on where they live. Participating rating authorities may review the experience and modify one or more of the ratings assigned after it is published to ensure the ratings are correct.

Parents and guardians can use Epic's Parental Controls to set content age rating limits based on their family's preferences. Parents can unlock specific islands that exceed the set ratings threshold using their Parental Controls PIN. There is also an option to turn on/off the ability for children to design their own games in Creative Mode.

24. Are there other areas in which we should consider potential future measures for the Children's Safety Codes?
- If so, please explain why and provide supporting evidence.

Developing the Children's Safety Codes: Our framework (Section 14)

25. Do you agree with our approach to developing the proposed measures for the Children's Safety Codes?
- If not, please explain why.
26. Do you agree with our approach and proposed changes to the draft Illegal Content Codes to further protect children and accommodate for potential synergies in how systems and processes manage both content harmful to children and illegal content?
- Please explain your views.

27. Do you agree that most measures should apply to services that are either large services or smaller services that present a medium or high level of risk to children?
28. Do you agree with our definition of 'large' and with how we apply this in our recommendations?
29. Do you agree with our definition of 'multi-risk' and with how we apply this in our recommendations?
30. Do you agree with the proposed measures that we recommend for all services, even those that are small and low-risk?
31. Do you agree with our proposal to recommend the use of highly effective age assurance to support Measures AA1-6? Please provide any information or evidence to support your views.
 - a. Are there any cases in which HEAA may not be appropriate and proportionate?
 - b. In this case, are there alternative approaches to age assurance which would be better suited?
32. Do you agree with the scope of the services captured by AA1-6?
33. Do you have any information or evidence on different ways that services could use highly effective age assurance to meet the outcome that children are prevented from encountering identified PPC, or protected from encountering identified PC under Measures AA3 and AA4, respectively?
34. Do you have any comments on our assessment of the implications of the proposed Measures AA1-6 on children, adults or services?
 - a. Please provide any supporting information or evidence in support of your views.

Age assurance measures (Section 15)

35. Do you have any information or evidence on other ways that services could consider different age groups when using age assurance to protect children in age groups judged to be at risk of harm from encountering PC?

Content moderation U2U (Section 16)

36. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.
37. Do you agree with the proposed addition of Measure 4G to the Illegal Content Codes?
 - a. Please provide any arguments and supporting evidence.

Search moderation (Section 17)

Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.

Are there additional steps that services take to protect children from the harms set out in the Act?

a. If so, how effective are they?

Regarding Measure SM2, do you agree that it is proportionate to preclude users believed to be a child from turning the safe search settings off?

The use of Generative AI (GenAI), see Introduction to Volume 5, to facilitate search is an emerging development, which may include where search services have integrated GenAI into their functionalities, as well as where standalone GenAI services perform search functions. There is currently limited evidence on how the use of GenAI in search services may affect the implementation of the safety measures as set out in this code. We welcome further evidence from stakeholders on the following questions and please provider arguments and evidence to support your views:

Do you consider that it is technically feasible to apply the proposed code measures in respect of GenAI functionalities which are likely to perform or be integrated into search functions?

What additional search moderation measures might be applicable where GenAI performs or is integrated into search functions?

User reporting and complaints (Section 18)

43. Do you agree with the proposed user reporting measures to be included in the draft Children's Safety Codes?
- Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence.
 - If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response.
44. Do you agree with our proposals to apply each of Measures UR2 (e) and UR3 (b) to all services likely to be accessed by children for all types of complaints?
- Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence.
 - If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response.
45. Do you agree with the inclusion of the proposed changes to Measures UR2 and UR3 in the Illegal Content Codes (Measures 5B and 5C)?
- Please provide any arguments and supporting evidence.

Terms of service and publicly available statements (Section 19)

46. Do you agree with the proposed Terms of Service / Publicly Available Statements measures to

be included in the Children's Safety Codes?

- a. Please confirm which proposed measures your views relate to and provide any arguments and supporting evidence.
 - b. If you responded to our illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response.
47. Can you identify any further characteristics that may improve the clarity and accessibility of terms and statements for children?
48. Do you agree with the proposed addition of Measure 6AA to the Illegal Content Codes?
- a. Please provide any arguments and supporting evidence.

Recommender systems (Section 20)

49. Do you agree with the proposed recommender systems measures to be included in the Children's Safety Codes?
- a. Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.
 - b. If you responded to our illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response.
50. Are there any intervention points in the design of recommender systems that we have not considered here that could effectively prevent children from being recommended primary priority content and protect children from encountering priority and non-designated content?
51. Is there any evidence that suggests recommender systems are a risk factor associated with bullying? If so, please provide this in response to Measures RS2 and RS3 proposed in this chapter.
52. We plan to include in our RS2 and RS3, that services limit the prominence of content that we are proposing to be classified as non-designated content (NDC), namely depressive content and body image content. This is subject to our consultation on the classification of these content categories as NDC. Do you agree with this proposal? Please provide the underlying arguments and evidence of the relevance of this content to Measures RS2 and RS3.

Please provide the underlying arguments and evidence of the relevance of this content to Measures RS2 and RS3.

User support (Section 21)

Do you agree with the proposed user support measures to be included in the Children's Safety Codes?

Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.

If you responded to our Illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior

22) Search features, functionalities and user support (Section 22)

Do you agree with our proposals? Please provide underlying arguments and evidence to support your views.

Do you have additional evidence relating to children's use of search services and the impact of search functionalities on children's behaviour?

Are there additional steps that you take to protect children from harms as set out in the Act?

a. If so, how effective are they?

As referenced in the Overview of Codes, Section 13 and Section 17, the use of GenAI to facilitate search is an emerging development and there is currently limited evidence on how the use of GenAI in search services may affect the implementation of the safety measures as set out in this section. We welcome further evidence from stakeholders on the following questions and please provide arguments and evidence to support your views:

Do you consider that it is technically feasible to apply the proposed codes measures in respect of GenAI functionalities which are likely to perform or be integrated into search functions? Please provide arguments and evidence to support your views.

Combined Impact Assessment (Section 23)

58. Do you agree that our package of proposed measures is proportionate, taking into account the impact on children's safety online as well as the implications on different kinds of services?

Statutory tests (Section 24)

Do you agree that our proposals, in particular our proposed recommendations for the draft Children's Safety Codes, are appropriate in the light of the matters to which we must have regard?

a. If not, please explain why.

Annexes

Impact Assessments (Annex A14)

In relation to our equality impact assessment, do you agree that some of our proposals would have a positive impact on certain groups?

In relation to our Welsh language assessment, do you agree that our proposals are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?

a. If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.

DRAFT