# Summary of our chapters

## Additional Safety Measures Statement

**Statement**

Published 16 November 2026

# About this document

This document includes a summary of each of the chapters included in the November 2026 Additional Safety Measures Statement.

# Chapter summaries

## 1. Introduction, our duties and navigating this Statement

### What is this chapter about?

This chapter provides a high-level overview of the statement, including its background, our duties and functions, and the wider UK Government policy and legislative context. It also explains the scope of this statement, how it operates, and the next steps.

## 2. Livestreaming

### What is this chapter about?

Livestreaming is a function where a user can create and distribute a live video that can be viewed by multiple other users. This chapter covers our full definition of livestreaming, explains the risks and benefits of it, and sets out our decisions on our proposed measures on reporting the risk of imminent physical harm on livestreams, the moderation of livestreams by humans, and protections for children using livestreaming functionality.

### What decisions have we made?

We have decided that livestreaming services should provide users with a mechanism to report livestreams depicting an imminent risk of physical harm, including of animal cruelty.

We have decided not to proceed with our proposal that services should ensure human moderators are available whenever users can livestream; we have also decided to suspend work on our proposal to restrict certain functionalities during children's livestreams.

We are proceeding with the following measure:

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU D17** | Livestreaming reporting mechanism for imminent physical harm | Providers of user-to-user services that:<br>a) have one-to many livestreaming; and<br>b) are at medium or high risk of one or more specified kinds of illegal harm. |

### Why have we made these decisions?

We consider that a dedicated reporting mechanism for imminent physical harm is a proportionate and effective way to help services identify and respond more quickly to serious illegal harms that can occur on livestreams. The measure will provide users with a clear means of reporting content that may involve an immediate risk of harm and support services in prioritising their response.

We have not proceeded with the proposed human moderation measure because we have concluded that existing content moderation measures within our Illegal Content Codes of Practice for user-to-user services already provide a proportionate and flexible basis for services to ensure moderation resourcing is appropriate to address the risks arising from livestreamed content.

We have decided to suspend work on the proposed children's livestreaming measure in light of the UK Government's announced plans, including restrictions on under-16s' access to social media and certain high-risk functionalities, including livestreaming. The Government's plans make the livestreaming proposals we had made unnecessary at this point in time.

## 3. User sanctions

### What is this chapter about?

This chapter sets out measures to ensure online services have effective and proportionate policies for sanctioning users who share, receive or view illegal content or content harmful to children. These sanctions include giving users warnings, suspensions or bans from a service, or restricting use of a service. The aim is to prevent repeat offending and reduce the future spread of harmful content online.

### What decisions have we made?

**Banning users for CSEA**

We have decided that providers of user-to-user services should ban users who generate, upload, share or receive and view child sexual exploitation and abuse (CSEA) content, including child sexual abuse material (CSAM and proxy content). Providers should prevent banned users from returning to a service, but we are not prescriptive about the technical methods used to do so.

For adult users, the default expectation is a permanent ban, except in extremely limited and exceptional circumstances.

Providers should treat children that share CSAM in a more nuanced way. Providers may decide not to ban children who shared sexual images of themselves because they were groomed, or exchanged images of themselves consensually within an age-appropriate relationship. In other cases involving child users, providers should impose bans that are proportionate to the circumstances.

**User sanctions policy**

We have decided that providers should prepare and apply a sanctions policy in respect of UK users who generate, upload, or share illegal content or content harmful to children which is prohibited on the service. We are not prescriptive about the sanctions they apply, and how they apply them, as long as they have regard to the factors set out in our measures: the severity of potential harm, whether the user has previously generated, shared or uploaded relevant content, and the potential impact of the sanction on the user.

We have also made a number of other amendments to existing code measures to complement these user sanctions measures.

Having considered our cost estimates and potential benefits, we have decided that these measures should no longer apply to providers of small, low risk services, or single risk providers.

Our final Code measures are summarised in the table below:

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU H3** | Banning users for CSEA | All user-to-user service providers. |
| **ICU H2** | User sanctions policy for illegal harms. | Providers of user-to-user services that are large and/or multi-risk for illegal harms. |
| **PCU H2** | User sanctions policy for content harmful to children. | Providers of user-to-user services likely to be accessed by children that are large and/or multi-risk for content harmful to children and prohibit one or more specific kinds of PPC, PC and/or NDC. |
| **ICU C4** | Set and record performance targets (for its content moderation function) | Providers of large and/or multi-risk user-to user-services where take down is not technically feasible. |
| **PCU C4** | | Providers of large and/or multi-risk user-to-user services which are likely to be accessed by children, where content and/or access level action is not technically feasible. |
| **ICU D8** | Set performance targets and resource itself to give effect to those targets for relevant complaints which are content appeals. | Providers of user-to-user services that are large and/or multi-risk for illegal harms. |
| **PCU D8** | | Providers of user-to-user services likely to be accessed by children that are large and/or multi-risk for content harmful to children and prohibit one or more specific kinds of PPC, PC and/or NDC. |
| **ICU D10** | Action following determination for relevant complaints which are content appeals. | All user-to-user service providers. |

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU D10A** | If a provider does not reverse a decision that content was illegal content or illegal content proxy following appeal (other than CSEA content or CSEA content proxy) but upholds, in whole or in part, a content appeal relating to the user being sanctioned, the provider should reverse the action taken against the user, and apply the appropriate sanction having regard to its sanctions policy. | Providers of user-to-user services that are large and/or multi-risk for illegal harms. |
| **PCU D10A** | If a provider does not reverse a decision that content was content harmful to children or content harmful to children proxy but upholds, in whole or in part, a content appeal relating to the user being sanctioned, the provider should reverse the action taken against the user and apply the appropriate sanction having regard to its sanctions policy. | Providers of user-to-user services likely to be accessed by children that are large and/or multi-risk for content harmful to children and prohibit one or more specific kinds of PPC, PC and/or NDC. |
| **ICU G1** | Include all information mandated by the Act in terms and statements including its policy on banning users in relation to CSEA content or CSEA content proxy. | All user-to-user service providers. |

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU G1A** | The provider should include in the terms of service provisions giving information about its policy on sanctions, addressing, at least, the sanctions which the provider may impose on users who generate, upload or share content that it determines to be illegal content and/or illegal content proxy, which is not CSEA content or CSEA content proxy. | Providers of user-to-user services that are large and/or multi-risk for illegal harms. |
| **PCU G1A** | The provider should include in the terms of service giving information about its policy on sanctions, addressing, at least, the sanctions which the provider may impose on users who generate, upload or share content that it determines to be relevant content that is harmful to children and/or content that is harmful to children proxy. | Providers of user-to-user services likely to be accessed by children that are large and/or multi-risk for content harmful to children and prohibit one or more specific kinds of PPC, PC and/or NDC. |

## Why have we made these decisions?

**Banning users for CSEA**

CSEA is a severe harm, and we consider that permanently removing adult offenders from services is a necessary and proportionate measure to mitigate this. The approach provides the strongest deterrent to future offending and offers the greatest protection to child users. A more nuanced approach to banning child users ensures that children are not unduly punished for sexual images they shared when they were groomed or for images shared within consenting age-appropriate relationships with another child.

**User sanctions policy**

Once content is identified as illegal or harmful to children through content moderation processes, there is an ongoing risk to users if no action is taken against the users who disseminated it. Without sanctions, there is also little deterrent to stop users from continuing to generate, upload and share this content.

These measures are therefore intended to prevent repeat violations and reduce the spread of harmful content by educating users, discouraging harmful behaviour and, where providers consider this appropriate, removing user access altogether.

# 4. Extending user controls

### What is this chapter about?

User controls include a range of functions to allow a user to control their interactions on online services, including functions such as user blocking, muting or disabling comments. In our April 2025 User Controls Consultation, we proposed expanding existing user control measures to include providers of certain smaller user-to-user services that are likely to be accessed by children, have relevant functionalities and are at risk of certain illegal harms.

The harms we seek to address include controlling or coercive behaviour, cyberflashing, harassment, stalking, threats and abuse, hate, grooming and encouraging or assisting suicide or serious self-harm.

### What decisions have we made?

We have decided to proceed with our proposed extension. Our final Code measures are summarised in the table below:

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU J1** | Service providers should offer every registered user the options to block and mute other user accounts on the service. | Providers of user-to-user services likely to be accessed by children that have user profiles, have at least one of user connections, posting content, and user communication, and have:<br><br>i) no more than seven million monthly UK users and high risk for at least one of grooming; encouraging or assisting suicide or serious self-harm; hate; harassment, stalking, threats and abuse; controlling or coercive behaviour; cyberflashing; or<br><br>ii) between 700,000 and seven million monthly UK users and medium risk for at least one of the relevant harms. |
| **ICU J2** | Providers of large user-to-user services should offer every registered user the option to disable comments on their content. | Providers of user-to-user services likely to be accessed by children that have the functionality of commenting on content, and have:<br><br>i) no more than seven million monthly UK users and high risk for at least one of grooming; encouraging or assisting suicide or serious-self harm; hate; harassment, stalking, threats and abuse; or<br><br>ii) between 700,000 and seven million monthly UK users and medium risk for at least one of the relevant harms. |

### Why have we made these decisions?

Functionalities including direct messaging, posting and commenting on content can be a risk factor for experiencing harms online. We know that user controls such as blocking, muting, and disabling comments are widely used by users to protect themselves from harm.

The extension of these measures to small services will significantly reduce the risk of child users being exposed to these illegal harms. Children will also be provided with clear information to help them understand what will happen if they implement these controls. This will empower children to control the content they see on services, who can contact them and who can interact with them, ensuring that children receive a higher standard of protection as required by the Act.

## 5. Highly effective age assurance in the Illegal Content Codes of Practice for user-to-user services

### What is this chapter about?

Under the Act, age assurance must be highly effective at correctly determining whether a user is an adult or a child. This chapter sets out our decisions to establish a consistent approach to highly effective age assurance across the Illegal Content and Protection of Children Codes, makes minor amendments to the Part 3 HEAA Guidance, and introduces measures on age-assessment appeals.

The measures support protections against serious illegal harms affecting children, including grooming and CSEA, by helping providers accurately determine which UK users are adults and apply appropriate safeguards to all remaining users.

The measures enable providers to use highly effective age assurance to target child-specific protections more effectively, while requiring safeguards, transparency, and appeals processes to ensure age-assurance systems are accurate, fair and proportionate.

### What decisions have we made?

We have decided to proceed with the proposed measures. Our final Code measures are summarised in the table below:

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU B1** | Use an age assurance process that meets the highly effective age assurance criteria (technical accuracy, robustness, reliability and fairness) and have regard to key implementation principles. | Providers of user-to-user services that use an age assurance process to determine which UK users are child users. |

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU D15** | Provide an age-assessment appeals process and take appropriate action where an appeal is upheld. | Providers of user-to-user services that use an age assurance process to determine which UK users are child users and that are large or multi-risk services. |
| **ICU D16** | Provide an age-assessment appeals process and take appropriate action where an appeal is upheld. | Providers of user-to-user services that use an age assurance process to determine which UK users are child users and that are neither large nor multi-risk services. |
| **PCU B1** | Amend the Protection of Children Codes to codify the highly effective age assurance criteria within the measure and align its structure with the Illegal Content Code. | Providers of user-to-user services likely to be accessed by children that use an age assurance process to determine which UK users are child users. |

### Why have we made these decisions?

These decisions will ensure providers that use age assurance have effective and consistent systems in place to determine which users are adults, enabling them to apply child-specific protections more accurately and consistently to all remaining users. This supports measures to prevent illegal harms affecting children, including grooming and CSEA, by ensuring that child-specific protections are provided for child users.

The measures are also designed to ensure that age assurance processes are accurate and transparent, and provide users with appropriate redress where their age has been incorrectly assessed. This should ensure that age assurance systems are fair and proportionate.

## 6. Increasing the effectiveness of safety defaults and supportive messaging

### What is this chapter about?

Our Codes state that, in order to protect children from grooming, children's accounts should have certain risky functionalities turned off by default. These functionalities include network expansion prompts, connection lists, location displays and certain direct messaging. In the June 2025 Additional Safety Measures Consultation, we proposed to amend the Codes to specify that, for the purposes of implementing these protections against grooming, service providers should either use highly effective age assurance or apply the measure to all users. This chapter explains our rationale to proceed with this amendment.

### What decisions have we made?

We have decided to proceed with the amendments. Our final Code measures are summarised in the table below:

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU F1**<br>**ICU F2** | When implementing safety defaults and supportive messaging as recommended by ICU F1 and ICU F2, providers should either:<br>i) use highly effective age assurance, as set out in the Part 3 HEAA Guidance to target the measures at child users; or<br>ii) apply ICU F1 and F2 to all users of the service | This is an amendment to measures ICU F1 and F2, therefore the measure will apply to:<br>a) regulated user-to-user services at high risk of grooming; and/or<br>b) regulated user-to-user services that are at a medium risk of grooming, and are a large service (7 million or more monthly UK users). |

### Why have we made these decisions?

Highly effective age assurance is a better way of determining which users are not determined to be adults than other methods such as self-declaration of age. This amendment to the Codes should therefore increase the proportion of children who benefit from protections against grooming.

## 7. Broadening content appeals

### What is this chapter about?

This chapter sets out our decision on technical changes that we have made to our Illegal Content and Protection of Children Codes relating to appeals. The changes are designed to extend users' rights of appeal against content moderation decisions. These act as a safeguard on users' freedom of expression.

### What decisions have we made?

Our final Code amendments are summarised in the table below:

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **Various ICU D measures**[1] | Broadening the scope of appeals measures to ensure that they cover decisions taken on the basis that content was an 'illegal content proxy' | Various (as set out in the amended measures). |

[1] ICU D2, D3, D4, D5, D6, D7, D8, D9, D10, D11, D12 and D13.

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **Various PCU D measures**[2] | Broadening the scope of appeals measures to ensure that they cover decisions taken on the basis that content was a 'content that is harmful to children proxy' | Various (as set out in the amended measures). |

### Why have we made these decisions?

These amendments will help ensure users can make content appeals when providers make moderation decisions by identifying proxy content. We consider that the amendments are appropriate and proportionate, as they protect users against excessive moderation and safeguard their rights to freedom of expression while having a limited impact on service providers.

## 8. Introduction to proactive technology

### What is this chapter about?

In this chapter we explain what proactive technology is and provide more detail about our constraints when making recommendations about proactive technology under the Act. We also respond to stakeholder feedback related to our overarching approach for proactive technology measures.

## 9. Deployment of proactive technology to detect image-based CSAM content

### What is this chapter about?

This chapter discusses the use of proactive technology[3] to detect previously unknown image-based child sexual abuse materials (CSAM).

**Proactive technology guidance**

Alongside this measure we are also publishing our draft proactive technology guidance to give service providers direction on how to implement proactive technologies.

### What decisions have we made?

We have decided to introduce a measure into our Codes of Practice[4] recommending service providers use recommended proactive technology for the purpose of detecting unknown image-based CSAM. We have assessed the degree of accuracy, effectiveness and lack of bias

[2] PCU D2, D3, D4, D5, D6, D7, D8, D9, D10, D13 and D14.
[3] Proactive technology describes technology that can be used as part of a content moderation system. The technology analyses content, user data and metadata to identify a range of outcomes including types of content, for example illegal content, user profiles, for example identifying user age, user behaviour, for example if a user is involved in illegal activity.
[4] Illegal Content Code of Practice for user-to-user services: Proactive Technologies (unknown content)

achieved by those technologies if configured and deployed to meet the proactive technology criteria we recommend.

We intend to consult on proactive technology for further harms in Spring 2027.

Our final Code measures are summarised in the table below:

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU PT1** | Deployment of proactive technology to detect image-based CSAM content. | Providers of:<br>a) Large user-to-user services at medium risk of image-based CSAM.<br>b) User-to-user services with more than 700,000 monthly active users in the UK at high risk of image-based CSAM.<br>c) File storage and file sharing services at high risk of image-based CSAM. |
| **ICU C4a** | Steps to take on reversal of content decisions. | All user-to-user services. |
| **PCU C4a** | Steps to take on reversal of content decisions. | All user-to-user services likely to be access by children. |
| **ICS C3A** | Steps to take on reversal of content decisions. | All search services. |
| **PCS C4A** | Steps to take on reversal of content decisions. | All search services likely to be accessed by children. |

### Why have we made these decisions?

Image-based CSAM can have a profound and long-lasting impact on children who are sexually abused, and on the wellbeing of individuals who encounter this content. The scale of online CSAM is increasing year on year,[5] and urgent action is needed to tackle this.

Our analysis shows that, when the recommended proactive technology meets the proactive technology criteria, it is capable in principle of being accurate, effective and lacking in bias in detecting image-based CSAM. The use of proactive technology should significantly increase the amount of CSAM that is detected and removed. This will help reduce the re-traumatisation of victims/survivors of abuse, improve law enforcement agencies' ability to disrupt ongoing abuse and reduce the risk of perpetrators abusing more children in future.

In response to stakeholder feedback, we have made the proactive technology measure more specific since the consultation and carried out a more detailed assessment of the accuracy and effectiveness of the technology.

[5] Internet Watch Foundation, 2025. Executive Summary, IWF Annual Data & Insights Report 2025.

# 10. Hash matching

## What is this chapter about?

Hash matching is technology used to detect known illegal or violative content. When a piece of content has been identified as being illegal, or violative, an identifier called a 'hash' (a string of identifying characters) is created to represent it and added to a database. A service then uses hash matching technology to identify content that matches the original hash. Techniques such as perceptual hashing can identify certain modified versions of content. This means the provider can either review the content or remove it automatically.

**Hash matching for terror content**

In this chapter we recommend the use of hash matching for terror content. We detail how this should be implemented, what constitutes an appropriate database and how human review should be utilised alongside hash matching.

**Hash matching for CSAM**

Our Illegal Content Codes for user-to-user services already recommend that certain service providers use hash matching to detect child sexual abuse materials (CSAM). We have decided to extend the existing hash matching measures for CSAM to include all services whose principal purpose is hosting or disseminating pornographic content, who are at high risk of image-based CSAM. We have made some changes to the provision on human review for all services to which the measure applies, to improve clarity and consistency.

**Hash matching guidance**

Alongside these measures, we have also updated our hash matching guidance to give service providers direction on how to implement hash matching measures.

## What decisions have we made?

We have decided to proceed with both measures. In our terror hash matching measure, we have made several amendments to improve clarity. Our final Code measures are summarised in the table below:

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU C13** | Services in scope should use hash matching technology to detect terrorism content. | User-to-user services that enable user-generated content in the form of photographs, videos and visual materials to be generated, shared or uploaded and are:<br>a) Large services at medium or high risk of terrorism content; or<br>b) At high risk of terrorism content and: i) have more than 700,000 monthly UK active users; or ii) are a file storage and file-sharing service. |

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU C9** | Deploy perceptual hash matching to detect known CSAM. | All high-risk services whose principal purpose is hosting or disseminating regulated pornographic content.[6] |

### Why have we made these decisions?

Hash matching is an effective way to identify content so that it can be moderated, or automatically taken down, depending on the type of illegal content.

**Hash matching for terror content**

This measure will increase the amount of terror content which service providers detect and remove. This will deliver significant benefits. Terror content is a serious and growing harm, and its availability can have severe real-world effects. Terrorism offences are often contextual; there might be legitimate reasons for sharing content related to terrorism, such as journalism. We have therefore included a number of safeguards in our measure to mitigate the risk of legitimate content being taken down inadvertently. We consider our measure strikes the correct balance in protecting users, but also ensuring that matched content is properly reviewed and, where appropriate, removed.

**Hash matching for CSAM**

Regardless of their size, there is a high risk of CSAM circulating on pornographic services. It is therefore essential that all pornographic services have robust safety systems, such as hash matching, in place. Our extension of the existing measure to detect CSAM will materially increase the amount of CSAM that is detected and removed from services. Given the severe and enduring damage CSAM does, this will deliver significant benefits.

## 11. Recommender systems

### What is this chapter about?

Recommender systems use an algorithm to curate personal content feeds and are often the primary method for users discovering new content on user-to-user services. However, recommender systems can also expose users to harmful and illegal content. If illegal content is not identified through moderation systems quickly, a recommender system may lead to the rapid spread of this content.

In our Protection of Children Code, we said that providers of in scope services should ensure that recommender systems exclude potential primary priority content from the feeds of any user who is not identified to be an adult using highly effective age assurance.

[6] Following our decisions in the December 2024 Statement on Protecting People from Illegal Harms (December 2024 Statement), this measure is already required by large services that are at medium or high risk of image-based CSAM; and by services that are at high risk of image-based CSAM and a) have more than 700,000 monthly active UK users or b) are file-storage and file-sharing services.

In this chapter, we set out our decision to proceed with measures to exclude content indicated to be potentially relevant illegal content[7] from children's recommender feeds.

### What decisions have we made?

In response to stakeholder feedback, we have amended our measure to target children's recommender feeds rather than all feeds. We have also decided not to apply the measure to foreign interference offences.

| Number in Codes | Recommended measure | Who should implement this |
|---|---|---|
| **ICU E3** | Content recommender systems: excluding potential relevant illegal content. | Services likely to be accessed by children that:<br>a) are at medium or high risk of suicide and self-harm; and<br>b) where a child-accessible part of the service has a content recommender system. |
| **ICU E2** | Content recommender systems: excluding potential relevant illegal content. | Services likely to be accessed by children that<br>a) are at medium or high risk of hate and/or<br>b) are medium or high risk of terrorism and<br>c) where a child-accessible part of the service has a content recommender system. |

### Why have we made these decisions?

This measure will reduce the risk of illegal content being recommended to children. By doing so, it should deliver important benefits to children.

## 12. Amendments to the Illegal Content Judgements Guidance for CSAM

### What is this chapter about?

Perpetrators use a range of online services, such as messages, group chats or forums, to facilitate the commission of offences involving child sexual abuse material (CSAM) and to share CSAM. In some cases, perpetrators of CSAM offences use the name, icon or bio / description on these services to indicate to other perpetrators that CSAM content can be found on part of the service (e.g. group chat or forum). This type of user data may be useful for service providers to identify perpetrators of CSAM on their services, particularly if they are unable to review the content of the users' messages, group chat or forum. This chapter sets out guidance to support service providers in assessing these types of information in

[7] Throughout the chapter, we have shortened to "potentially relevant illegal content" to "potentially illegal content."

order to determine whether it is reasonable to infer that a messaging thread, group chat or forum exists for the purposes of committing CSAM offences.

### What decisions have we made?

We have amended the Illegal Content Judgements Guidance (ICJG) to support service providers in making judgements about illegal content when they are unable to review messages, group chats, or forums.

To do this, we have set out three scenarios that illustrate how a provider can infer that content is illegal and explain our reasoning in this chapter.

### Why have we made these decisions?

These scenarios will support service providers to identify and reduce the spread of CSAM on their services. As a result, this guidance directly contributes to the protection of survivors and victims of child sexual abuse.

## 13. Combined impact assessment

### What is this chapter about?

In the preceding chapters of this statement, we assess the individual impact of each of the decisions we have taken in terms of new Code measures or amendments to the Codes. In this chapter, we assess the combined impact of the measures as a package, including their expected impact on economic growth. Having considered the combined impact on different groups of services and on economic growth, we explain why we have determined that the package of measures is proportionate.

## 14. Statutory tests

### What is this chapter about?

In designing the Codes, the Online Safety Act 2023 (the Act) requires Ofcom to have regard to a number of principles and objectives, set out in Schedule 4 to the Act. The Communications Act 2003 (the 2003 Act) also places a number of duties on Ofcom in carrying out our functions.
In this chapter, we set out the matters to which we must have regard under the Act and the 2003 Act, and explain the reasons why we think the recommendations in the Codes meet them.