Annex 1: Further stakeholder responses

Additional Safety Measures Statement

Statement Annex

Published 16 November 2026

For more information on this publication, please visit ofcom.org.uk

Contents

A0. Further stakeholder responses 3

A1. Introduction, our duties and navigating the Statement 4

A2. Livestreaming 22

A3. User sanctions 41

A4. Extending user controls 58

A5. Highly effective age assurance in the Illegal Content Codes 70

A6. Increasing the effectiveness of safety defaults and supportive messaging 78

A7. Broadening content appeals 88

A8. Introduction to proactive technology 94

A9. Deployment of proactive technology to detect image-based CSAM 100

A10. Hash matching 106

A11. Recommender systems 124

A12. Amendment to the Illegal Content Judgements Guidance (ICJG) for CSAM 133

A13. Combined impact assessment 138

A0. Further stakeholder responses

Warning: this annex contains content that may be upsetting or distressing.

About this annex

A0.1 This annex addresses the additional points that were made by respondents to our April 2025 Illegal Harms Further Consultation: User Controls and June 2025 Additional Safety Measures Consultation.

A0.2 While we have reviewed all the relevant feedback, we did not consider that the points set out in this annex required substantial additions or explanations in our statement. We have considered all stakeholder responses received even where we have not referred to or quoted them in the statement or this annex.

A1. Introduction, our duties and navigating the Statement

Stakeholder responses by theme

Feedback on Ofcom's approach

Speed of approach

A1.1 The Commissioner Designate for Victims of Crime in Northern Ireland welcomed our iterative approach, noting it was necessary to keep pace with fast-changing technology.[1] South West Grid for Learning (SWGfL) also noted our improved engagement and iteration.[2]

A1.2 Several industry and civil society stakeholders said that our incremental approach to regulation was too fast.[3] They variously said this raises risks including poor implementation, data leaks, [✂]. X said that it would be premature and potentially disproportionate to introduce additional measures before Ofcom has robustly assessed the effectiveness and impact of the existing Codes.[4] techUK raised concerns about the timing of the consultation, which proposed additional measures before the Protection of Children Codes had come into force and shortly after the Illegal Content Codes took effect. techUK said this did not allow time to gather evidence on the effectiveness, costs or operational impact of the existing Codes, and recommended that Ofcom gather data on their impact before introducing new measures.[5]

A1.3 A number of stakeholders said that our iterative approach was too slow.[6] These stakeholders said this caused a range of issues including Codes not keeping pace with emerging technologies and harms, divergence from best practice, leaving users exposed to well-evidenced risks for too long, a lack of parity between the Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes) and Protection of Children Code of Practice for user-to-user services (Protection of Children Code), and an underdeveloped protection for harms such as suicide, self-harm, or harms relating to livestreaming. Two civil society stakeholders noted the length of time between the June 2025 Additional Safety Measures Consultation (June 2025 Consultation) and the Illegal Content and Protection of Children Codes coming into force.[7]

---

[1] Commissioner Designate for Victims of Crime in Northern Ireland response to the June 2025 Consultation, p.3.
[2] Southwest Grid for Learning (SWGfL) response to the June 2025 Consultation, p.3.
[3] [✂]; Open Rights Group Campaign response to the June 2025 Consultation, p.6; [✂]; [✂].
[4] X response to the June 2025 Consultation, p.1.
[5] techUK response to the June 2025 Consultation, p.2;
[6] 5Rights Foundation response to the June 2025 Consultation, p.1; Centre for Countering Digital Harm (formerly Centre for Countering Digital Hate) (CCDH) response to the June 2025 Consultation, p.3-4; [✂]; Marie Collins Foundation response to the June 2025 Consultation, pp.14-15; Molly Rose Foundation response to the June 2025 Consultation, p.3; Refuge response to the June 2025 Consultation, p.1; SWGfL response to the June 2025 Consultation, p.3.
[7] Molly Rose Foundation response to the June 2025 Consultation, p.3; Refuge response to the June 2025 Consultation, p.1.

Regulatory uncertainty

A1.4 Industry stakeholders raised the importance of regulatory certainty,[8] with several stakeholders calling for a period of stability, or roadmap for future changes.[9] Stakeholders said introducing new measures too quickly meant we could not properly assess the proportionality of proposed measures.[10]

A1.5 Two respondents said that this uncertainty led to higher costs than we recognised.[11]

A1.6 A government stakeholder recommended we set out a schedule of updates and work more closely with the UK Government in the development of Codes to allow government departments to feed in evidence around evolving threats.[12]

Regulatory overreach

A1.7 The Open Rights Group Campaign and an individual stakeholder said our measures amounted to regulatory overreach and scope creep.[13] The Open Rights Group Campaign argued that Ofcom lacks the authority for these measures.

Ambition of additional safety measures

A1.8 Civil society and public body stakeholders said that Ofcom should be more ambitious on issues including scope, technological advances, tone of language and agility.[14]

A1.9 In particular, stakeholders called for a more ambitious approach to tackling harms relating to fraud, violence against women and girls (VAWG), and suicide and self-harm, eating disorder and depression content.[15]

Flexibility of approach

A1.10 Two industry stakeholders said Ofcom should avoid being overly prescriptive and allow services to adopt context appropriate processes that are outcome focussed.[16]

---

[8] Computer and Communications Industry Association (CCIA) response to the June 2025 Consultation, p.16; Google LLC response to the June 2025 Consultation, p.1; [✂]; Online Dating and Discovery Association (ODDA) response to the June 2025 Consultation, p.10; [✂]; [✂]; Twitch response to the June 2025 Consultation, p.18; [✂]; [✂]; Yoti response to the June 2025 Consultation, p.22.

[9] [✂]; [✂].

[10] Google LLC response to the June 2025 Consultation, p.1; ODDA response to the June 2025 Consultation, p.10; [✂]; [✂]; [✂]; [✂].

[11] Google LLC response to the June 2025 Consultation, p.1; [✂].

[12] [✂].

[13] Cook J response to the June 2025 Consultation, p 1; Open Rights Group Campaign response to the June 2025 Consultation, p.6.

[14] 5Rights Foundation response to the June 2025 Consultation, pp.1-2; Lucy Faithfull Foundation response to the June 2025 Consultation, p.11; Marie Collins Foundation response to the June 2025 Consultation, p.14-15; Molly Rose Foundation response to the June 2025 Consultation, p.1; National Society for the Prevention of Cruelty to Children (NSPCC) response to the June 2025 Consultation, p.2,9; Online Safety Network (new name) response to the June 2025 Consultation, pp.3-5. Online Safety Network (OS Network) formerly Online Safety Act Network (OSA Network), changed its name since the June 2025 Consultation. We will refer to them by their new name for the remainder of the statement; Refuge response to the June 2025 Consultation, p.2; Scottish Government response to the June 2025 Consultation, p.4.

[15] Domestic Abuse Commissioner for England and Wales response to the June 2025 Consultation, p.8; Refuge response to the June 2025 Consultation, p.16; University College London (UCL) Gender and Tech Research Lab (Institute for Engineering and Technology (IET)) response to the June 2025 Consultation, p.1.

[16] Middle Tech Coalition response to the June 2025 Consultation, pp 2-3; [✂].

A1.11 Whereas, SWGfL said Ofcom placed too much emphasis on cost to services and flexibility and should focus more on user rights and harm prevention.[17]

Safety by design

A1.12 A number of civil society stakeholders, public bodies, and one academic stakeholder highlighted the importance of safety by design.[18] This included noting the principles that a safety by design approach should encompass including survivor inclusion, co-design and abusability testing.[19]

A1.13 Several stakeholders said our approach was reactive and that measures should focus on perpetrators and the prevention of harm.[20] The Online Safety Network (OS Network) and the Molly Rose Foundation noted that measures detect harms after they have occurred and argued that Ofcom should do more to ensure upstream prevention.[21]

A1.14 Several stakeholders highlighted the importance of service providers taking responsibility for user safety including annual testing, bug bounty programmes and identifying software vulnerabilities.[22]

Accessibility of the June 2025 Consultation

A1.15 Several individuals, civil society stakeholders, and public body stakeholders raised issues with the consultation questions, the language used, and the response form.[23] They stated that the number of questions, technical language, and the response form itself created a barrier to a wider audience responding.

Our response

Speed, regulatory uncertainty and ambition

A1.16 We acknowledge the challenge of balancing a regulatory environment that is suitably stable but accounts for the severity of online harms and speed of technological developments. Stakeholders expressed differing views on this balance, with some considering that we are moving too quickly and others that we should move more quickly. We recognise that striking this balance will be an ongoing challenge and we will keep this under review.

---

[17] South West Grid for Learning response to the June 2025 Consultation, p. 3.
[18] Common Sense Media response to the June 2025 Consultation, p.6; Domestic Abuse Commissioner response to the June 2025 Consultation, p.7-8; FCA UK response to the June 2025 Consultation, p.1; Glitch response to the June 2025 Consultation, p.5; Lucy Faithfull Foundation response to the June 2025 Consultation, p.2; Marie Collins Foundation response to the June 2025 Consultation, p.13; SWGfL response to the June 2025 Consultation, p.3; The Children's Commissioner's Office (CCO) response to the June 2025 Consultation, p.20; [✂]; UCL Gender and Tech Research Lab (IET) response to the June 2025 Consultation, p.5.
[19] UCL Gender and Tech Research Lab (IET) response to the June 2025 Consultation, p.5.
[20] CCO response to the June 2025 Consultation, p.20; Lucy Faithfull Foundation response to the June 2025 Consultation, p.2; Marie Collins Foundation response to the June 2025 Consultation, p.13; Molly Rose Foundation response to the June 2025 Consultation, pp.3-4; NPCC response to the June 2025 Consultation, p.4; Online Safety Network response to the June 2025 Consultation, p.12; SWGfL response to the June 2025 Consultation, p.3; [✂].
[21] Molly Rose Foundation response to the June 2025 Consultation, pp.3-4; Online Safety Network (OS Network) response to the June 2025 Consultation, p.12.
[22] Antisemitism Policy Trust response to the June 2025 Consultation, p.5; CCO response to the June 2025 Consultation, p.20; Common Sense Media response to the June 2025 Consultation, p.6; Full Fact response to the June 2025 Consultation, p.4; Scottish Government response to the June 2025 Consultation, p.4; [✂].
[23] [✂]; Domestic Abuse Commissioner response to the June 2025 Consultation, p.3; [✂]; Scottish Government response to the June 2025 Consultation, p.1.

A1.17 While we acknowledge stakeholder concerns that the approach to new Codes measures has been fast, the nature and speed with which online harms are progressing means there is a need to balance speed with the regulatory process.

A1.18 There is clear evidence of the need to bolster initial Codes through these additional measures. This evidence is set out throughout the statement.

A1.19 We have aimed to ensure that the regulatory environment is suitably stable – for example, by giving notice of the June 2025 Consultation in the December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement) and the April 2025 Statement on Protecting Children from Harms Online (April 2025 Statement). However, given the scale and severity of the harms we deal with, we need to ensure users, in particular children, are appropriately protected from harm at the earliest juncture.

A1.20 In response to those stakeholders who state we should move more quickly, we are ensuring the statutory regulatory process is being followed for highly complex and detailed work and are reviewing processes for opportunities to make these faster and more efficient.

A1.21 Given the nature of online harms, producing a long-term roadmap is challenging. We publish annual roadmaps which provide updates on the remaining implementation steps for the regime. Our industry roadmap provides an ongoing, up to date outline of the remaining steps for the implementation of the regime. Our current roadmap outlines activities to May 2027.[24]

A1.22 The roadmap focuses on when we will deliver the Codes, guidance and statutory reports, and advice to the Secretary of State that is required under the Act. It will also include work to respond to new legislation. However, this does not show our ongoing work to drive compliance and monitoring online harms across the industry.

Flexibility of approach

A1.23 Ofcom have a duty to have regard to the principle that measures in Codes must be sufficiently clear and at a sufficiently detailed level, that service providers understand what the measures entail in practice. We are also required to impact assess the measures which means we have to set out our thinking on the costs as well as the benefits of the measures. We have afforded service providers flexibility where we consider it appropriate and proportionate to do so to achieve a measure's objective.

A1.24 Service providers may comply with their safety duties through alternative means. If using alternative measures, providers must keep a record of what they have done and how this meets relevant safety duties. In adopting alternative measures, providers should have regard to the importance of users' rights to freedom of expression within the law, and the right to privacy.

Safety by design

A1.25 The term 'safety by design' can be interpreted in various ways, but for the purpose of this statement we use it to mean a proactive approach to integrating safety considerations into the design cycle of products, systems, or processes. This includes making iterative improvements to existing systems on longstanding services or features. It also can include retirement (replacing or removing a feature or functionality altogether), as well as ensuring new services or features are designed with safety in mind from the outset.

[24] Ofcom (2026), Ofcom's approach to implementing the Online Safety Act.

A1.26 We agree with stakeholders that safety by design is an essential part of online safety, as outlined by the 2025 UK Government priorities. The duty on providers to carry out a suitable and sufficient risk assessment includes, when appropriate, the need to carry out testing before making a significant change to any aspect of a service's design or operation.[25]

A1.27 We consider that many features of our overall package of measures promote safety by design. The December 2024 and April 2025 Statements establish baseline protections from illegal content and content harmful to children. This statement builds on these protections.

A1.28 We agree with stakeholders that it is important for providers to continue to innovate and to develop new safety technologies. We note that evidence suggests that children want safer online experiences, which means that taking user safety seriously is not just of benefit to users, but also to service providers.[26]

A1.29 We expect to learn more about innovating practices adopted by service providers through our supervision work and monitoring and evaluation.

Accessibility of the consultation

A1.30 Our consultations are necessarily detailed due to our legal obligations to provide stakeholders with sufficient detail to enable an informed response. We are required to consult on our assessment of the likely impact of proposals which would be likely to have a significant impact on businesses or the general public, or when there is a major change in Ofcom activities under section 7 of the Communications Act 2003.

A1.31 To make our consultation more accessible to those concerned, we undertook a workshop with individuals with lived experience which aimed for individuals to be able to share their feedback on the June 2025 Consultation. We have taken this feedback into account in reaching our decisions.

A1.32 We also invited stakeholders to attend roundtables on the different measures. These roundtables allowed stakeholders to ask questions and speak about the measures with other stakeholders, which in turn fed into their consultation responses. We aim to continue thinking of more innovative ways to improve the consultation process and roll these out in our future work.

A1.33 The June 2025 Consultation also integrated accessible tables within the document (June 2025 Consultation, chapter 2: Summary of our proposals).

A1.34 We have created two separate, accessible versions of the decisions taken in this statement which can be found on the Ofcom website. This includes a summary of our chapters which sets out a high-level summary of each chapter in our statement; and a summary of our decisions which includes tables outlining our decisions and which services they apply to.

A1.35 We set out in the June 2025 Consultation that it was not necessary to use the response form, and we considered responses submitted outside of this format with equal weight.

[25] Sections 9 and 26 of the Online Safety Act 2023; Ofcom (2026), Risk Assessment Guidance and Risk Profiles, p.10 and p.23.
[26] Ofcom (2025), Consulting children on Protection of Children Online Safety Proposals.

Data protection and the Information Commission's Office (ICO) response

A1.36 The Information Commission's Office (ICO)[27] welcomed our commitment to data protection compliance and noted that services must comply with data protection law when implementing measures.[28] It suggested Ofcom provide a detailed overview of all the measures considered to be privacy safeguards and the extent to which we refer to measures that might act as data protection safeguard, but not privacy safeguards.[29]

Our response

A1.37 We agree that service providers need to comply with data protection and privacy laws, as they do all other applicable UK laws, when complying with the Act. Ofcom is not the data protection regulator, so to understand how data protection law applies to their services, service providers should have regard to relevant ICO guidance.

A1.38 Ofcom's duty under the Act is to design measures having regard to the importance of protecting the privacy of users.[30] This is a reference to protecting users from a breach of "any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a user-to-user service or a search service (including, but not limited to, any such provision or rule concerning the processing of personal data)".

A1.39 Not all of data protection law concerns privacy. However, in considering the privacy impacts of our recommendations, we have had regard to the duties service providers have under data protection law. Where a principle of data protection appears particularly relevant, we have discussed it even when it is not clear that it concerns privacy. However, we have not attempted to discuss every aspect of data protection law which may be relevant to our proposals.

A1.40 In general, we consider the application of data protection principles and duties helps to safeguard the right to privacy. For further details see chapter 1: Introduction, our duties and navigating the statement and chapter 14: Statutory test.

Technical feasibility

A1.41 A number of civil society and public body stakeholders raised concerns about the use of 'technical feasibility' throughout the proposed measures, stating that this could create a 'get-out clause' to claim compliance without implementing measures.[31] One stakeholder

[27] The Information Commission's Office (ICO), formerly the Information Commissioner's Office, changed its name since the June 2025 Consultation. We will refer to them by their new name for the remainder of the Annex.
[28] ICO response to the June 2025 Consultation, p.2.
[29] ICO response to the June 2025 Consultation, p.13.
[30] Schedule 4 paragraph 10.
[31] Barnardo's response to the June 2025 Consultation, p.7; CCO response to the June 2025 Consultation, p.8; Domestic Abuse Commissioner response to the June 2025 Consultation, pp.1-2, 5; Internet Watch Foundation (IWF) response to the June 2025 Consultation, pp.11, 12, 16, 17, 29, 30; Marie Collins Foundation response to the June 2025 Consultation, p.13; NSPCC response to the June 2025 Consultation, pp.25, 33; Online Safety Network response to the June 2025 Consultation, pp.12-13; Refuge response to the June 2025 Consultation, p.6; SWGfL response to the June 2025 Consultation, pp.2, 10; UCL Gender and Tech Research Lab (IET) response to the June 2025 Consultation, p.2; UK Finance response to the June 2025 Consultation, pp.2, 7;

called for the removal of the technical feasibility clause, with another calling it "a loophole".[32]

A1.42 Several stakeholders referenced a blog by the Online Safety Network (OS Network) raising concerns that providers would use technical feasibility to "simply opt out of finding innovative solutions to prevent harm."[33]

A1.43 [✂].[34] Mega noted that, because its service is end-to-end encrypted, it is not technically feasible to apply hash matching at the point of upload, and that such measures can only be applied once content has been reported to it.[35]

A1.44 Mega highlighted inconsistencies in the June 2025 Consultation on technical feasibility including Measure ICU C11 being worded differently in chapters 2 and 9, and the qualification being listed in annex 14 but not relevant chapters. It recommended the qualification be included consistently in all relevant sections and measures.[36]

A1.45 Stakeholders noted the importance of technical feasibility being enforceable for the success of measures.[37] Several civil society stakeholders welcomed Ofcom's decision to investigate feasibility claims but requested clarity on how these would be assessed and the documentation service providers must keep.[38]

A1.46 Stakeholders suggested that Ofcom should require evidence to demonstrate that a proposal is infeasible.[39] They said this should be reviewed alongside technological advancements, with the method used to make our assessment and configuration choices published. International Justice Mission said that, given the proven efficacy of proactive technologies, Ofcom should treat claims of infeasibility with scepticism and be ready to take enforcement action on this.[40]

Costs and technical feasibility

A1.47 A number of civil society and public body stakeholders called for clarity that high costs is not an adequate reason for a service provider to claim technical infeasibility.[41]

---

[32] Marie Collins Foundation response to the June 2025 Consultation, p.13; SWGfL response to the June 2025 Consultation, p.2.
[33] Refuge response to the June 2025 Consultation, p.6; SWGfL response to the June 2025 Consultation, pp.2, 10: Online Safety Network, 2025; Requirements for OSA Codes measures: technical feasibility and proportionality – Online Safety Act.
[34] [✂].
[35] Mega response to the June 2025 Consultation, pp.8-9, pp.17-18.
[36] Mega response to the June 2025 Consultation, pp.8-9, 17-18.
[37] Domestic Abuse Commissioner response to the June 2025 Consultation, pp.1, 2 ,5; Yoti response to the June 2025 Consultation, p.23.
[38] Barnardo's response to the June 2025 Consultation, p.7; IWF response to the June 2025 Consultation, pp.11-12; Marie Collins Foundation response to the June 2025 Consultation, p.13; Online Safety Network response to the June 2025 Consultation, pp.12-13; [✂].
[39] NSPCC response to the June 2025 Consultation, p.25; SWGfL response to the June 2025 Consultation, p.2.
[40] IJM response to the June 2025 Consultation, p.10.
[41] CCO response to the June 2025 Consultation, p.3; IWF response to the June 2025 Consultation, p.17; Online Safety Network response to the June 2025 Consultation, pp.12-13; SWGfL response to the June 2025 Consultation, p.2; UCL Gender and Tech Research Lab (IET) response to the June 2025 Consultation, p.2.

Our response

A1.48 The Act requires Ofcom to have regard to the principle that "the measures described in the Code of Practice must be proportionate and technically feasible," and to consider how the size, capacity and kind of service may impact technical feasibility.[42]

A1.49 Where a service provider claims that a measure is technically infeasible, Ofcom has the powers to investigate this.

A1.50 We may consider factors including:

a) the type of service;
b) the functionalities of the service;
c) the architecture and technical design of the service;
d) the effectiveness of the technology; and
e) the technical requirements for implementation and use of technology.

A1.51 We have updated the relevant measures accordingly.

Costs and technical feasibility

A1.52 We acknowledge that cost might be a barrier to implementing some kinds of technology. Our proportionality assessment considered costs and impacts on services – including on different types of services – in determining which measures to recommend and the benefits to users from improving the safety of services.

A1.53 We agree that high costs do not mean that a measure would be technically infeasible to implement. Additionally, requiring some changes to be made to the design or operation of the service would not mean a measure is technically infeasible. The Act considers the size and capability of a service as part of technical feasibility, and we will take this into consideration on a case-by-case basis when assessing if a measure is technically feasible for a service.

End-to-end encryption

A1.54 The European Digital Rights Organisation and an individual stakeholders disagreed with applying measures to end-to-end encrypted services, stating this would harm privacy and that client-side scanning was "not safe, secure or feasible".[43]

Our response

A1.55 There is mixed feedback on how measures should apply in these environments, we note that all services need to adhere to the duties in the Act. Our recommendations on proactive technology only apply to publicly communicated content.

Virtual private network (VPN) usage and riskier services

A1.56 Civil society, individual and public body stakeholders said that the measures would increase the use of virtual private networks (VPNs) and users moving to riskier services online.[44] Several stakeholders cited news reports of that quoted Proton VPN saying they

[42] The Act Schedule 4, Section 42, 2c.
[43] European Digital Rights Organisation response to the June 2025 Consultation, p 1; Thompson, A. response to the June 2025 Consultation, p. 3.
[44] Antisemitism Policy Trust response to the June 2025 Consultation, p.5; Barnardo's response to the June 2025 Consultation, p. 17; Computer and Communications Industry Association (CCIA) response to the June 2025 Consultation, p.14; Name Withheld 4 response to the June 2025 Consultation, p.11; [✂]; Name Withheld 11 response to the June 2025 Consultation, p.1; Name Withheld 26 response to the June 2025 Consultation, p.9;

had an increase in the use of VPNs since the introduction of highly effective age assurance.[45]

A1.57 The British and Irish Law Education Technology Association (BILETA) raised the risk of offenders migrating to end-to-end encrypted services. It cited evidence such as the 40% drop in CSAM reports after end-to-end encryption rollout.[46]

Our response

A1.58 In July 2026 we published our Use of Age Assurance Report.[47] In this, we found that circumvention of age assurance appears low, with a relatively small minority of children reporting that they circumvent highly effective age checks or use VPNs to access restricted content of features. However, some activity may not be captured due to reporting bias.

A1.59 Our evidence suggests that VPN use increased among UK users, but does not currently show that this increase is due to children motivated by a desire to bypass age checks on online services. Evidence on circumvention techniques is limited but indicates that robust configuration and monitoring of age assurance processes is important to mitigate known and emerging risks.[48] Our highly effective age assurance guidance is clear that services must not direct or encourage users to circumvent age assurance, including through the use of VPNs.[49]

A1.60 We will continue to monitor VPN usage and develop our evidence base on circumvention and displacement, but it would be a matter for the government to decide whether to take steps to address VPN usage by children.

A1.61 We acknowledge that some users might move to end-to-end encryption services. However, we are confident that our measures make users materially safer.

Generative artificial intelligence (AI)

A1.62 Civil society stakeholders raised concerns about the harms of generative artificial intelligence (AI), including the risks of chatbots, generating hyper-realistic and illegal or harmful content and disinformation.[50] Stakeholders argued that Ofcom should address emerging threats and align with international standards, including TAKE IT DOWN Act in the US and California's AI Child Abuse Material Law.[51]

Our response

A1.63 Content generated using AI can be in scope of the Act. AI-generated content shared by users on a user-to-user service is classed as user-generated content and would be regulated in the same way as content generated by humans. This means that when providers of user-to-user services become aware of AI-generated content that is illegal

---

[✂]; NPCC response to the June 2025 Consultation, p.13; Open Rights Group Campaign response to the June 2025 Consultation, p.6; Scottish Government response to the June 2025 Consultation, p.2; Tariq, F. response to the June 2025 Consultation, p.2.

[45] BBC, July 2025. VPNs top App Store charts as UK age verification kicks in – BBC News.

[46] British and Irish Law Education Technology Association (BILETA) response to the June 2025 Consultation, pp.39-40.

[47] Ofcom (2026), Use of Age Assurance, p.48; Ofcom (2026), Children's use of VPNs.

[48] Ofcom (2026), Use of Age Assurance, p.61.

[49] Ofcom (2025), Guidance on highly effective age assurance, p.16.

[50] Antisemitism Policy Trust response to the June 2025 Consultation, p.5; BILETA response to the June 2025 Consultation, p.39; Common Sense Media response to the June 2025 Consultation, p.7; National Society for the Prevention of Cruelty to Children (NSPCC) response to the June 2025 Consultation, p.20, pp.30-32.

[51] Common Sense Media response to the June 2025 Consultation, p.7.

content or content harmful to children, they should take swift, appropriate action. Similarly, AI-generated content which is search content would be regulated in the same way as content generated by humans on a regulated search service.

A1.64 The Act regulates user-to-user services, search services, and services that publish pornographic content. As such, chatbots are not subject to regulation if they:

a) only allow people to interact with the chatbot itself and no other users (and are therefore not a user-to-user service);
b) do not search multiple websites or databases when giving responses to users (and are therefore not a search service); and
c) cannot generate pornographic content.

Proportionality

A1.65 Two stakeholders disagreed with our proportionality assessment.[52]

Industry resource

A1.66 Several stakeholders said the industry resources required to address harm should be proportionate to service size and risk of harm to achieve the greatest harm reduction.[53]

Risk levels

A1.67 The Marie Collins Foundation said Ofcom acknowledged that risk could transfer to smaller services but still relied on risk matrices and thresholds that tolerate ongoing harm.[54] It asked Ofcom to change its stance on risk matrices, even if this requires changes to the Act.

Impact on small services

A1.68 Individual respondents, civil society stakeholders, and an industry stakeholder raised the potential disproportionate impact of the measures on small services and creators, saying requirements should be proportionate to the size of service, function and risk profile.[55] Respondents said small service providers would struggle with the cost of implementing measures, including moderation,[56] the accessibility of documentation, and need for lawyers to interpret this.[57] They said small UK businesses could suffer, and this could lead to monopolies.[58]

A1.69 Conversely, Demos and Barnardo's mentioned the need for small services to implement measures, noting that illegal content can originate on small services.[59]

---

[52] BILETA response to the June 2025 Consultation, p.42; [✂].
[53] BILETA response to the June 2025 Consultation, p.41; [✂].
[54] Marie Collins Foundation response to the June 2025 Consultation, p.13.
[55] Name Withheld 11 response to the June 2025 Consultation, p.2; Open Rights Group Campaign response to the June 2025 Consultation, p.3; Tariq, F. response to the June 2025 Consultation, p.1; [✂]; Together Declaration Campaign response to the June 2025 Consultation, p.5.
[56] Name Withheld 11 response to the June 2025 Consultation, p.2; Tariq, F. response to the June 2025 Consultation p.1; Together Campaign Declaration Campaign response to the June 2025 Consultation, p.5.
[57] Open Rights Group Campaign response to the June 2025 Consultation, p.3.
[58] Francis, S. response to the June 2025 Consultation, pp.3-4; Name Withheld 11 response to the June 2025 Consultation, p.2; Together Declaration Campaign response to the June 2025 Consultation, p.5.
[59] Barnardo's response to the June 2025 Consultation, p.11; Demos response to the June 2025 Consultation, p.32.

Evidential thresholds

A1.70 Civil society stakeholders said proportionality and evidential thresholds were too high.[60] One industry stakeholder said we should assess the evidence of existing actions before implementing new measures.[61] Stakeholders argued the risk to users of inaction and severity of potential harms, should be factored into proportionality.[62] UK Finance called for transparent statistics to drive best practice.[63]

Our response

A1.71 We acknowledge that imposing costs on providers can have negative impacts or risks for users. This might include service providers ceasing operations in the UK or reduced innovation. While there may be a loss to users, this may be in users' overall interest if such services are causing significant harm through illegal content and if providers are not prepared (or cannot afford) to apply a measure to sufficiently address that harm.

A1.72 We are required under the Act to consider the proportionality of measures (having regard to the size and capacity of the provider) and to carry out an impact assessment which includes an assessment of impacts on small and micro businesses.[64] For each of our measures we have assessed the proportionality of measures (including the cost to action and maintain them) particularly with regard to the impact on small services. We have also assessed the cumulative impact of our measures, with a particular focus on small services, in chapter 13: Combined impact assessment.

A1.73 The severity of the harms being addressed means that we cannot tackle these with no impact on service providers. However, we consider that we have struck the right balance within our measures. When deciding who each measure applies to, we have considered where there are the greatest risk of harms and the proportionate action needed to address harms for these services. This means that measures do not apply to small services where, in our view, the cost is not justified to produce sufficient benefits.

A1.74 The acceptable risk levels are determined alongside the severity of potential harms and subsequent impacts on users and service providers. We acknowledge that these might lead to a negative impact on growth and innovation in some cases.[65] However, we consider that the package of measures that we are proposing in this statement is proportionate to those they apply to, and that any negative impact it may have on a provider or creator is proportionate to the risk of harm to users.

Evidential thresholds

A1.75 The Act contains a series of matters to which Ofcom must have regard, and tests that we must meet, before we can make recommendations in Codes. Ofcom is not entitled to recommend measures which we have not specified in sufficient detail, impact assessed and determined to be proportionate. Protecting people from harm is central to our decision

---

[60] Molly Rose Foundation response to the June 2025 Consultation, pp.1,11; SWGfL response to the June 2025 Consultation, pp.2,3.
[61] Google LLC response to the June 2025 Consultation, p.1.
[62] Marie Collins Foundation response to the June 2025 Consultation, p.13; National Policy Chiefs' Council (NPCC) letter response to the June 2025 Consultation, p.2; SWGfL response to the June 2025 Consultation, pp.2,3.
[63] UK Finance response to the June 2025 Consultation, p.18.
[64] Paragraph 2(c) of Schedule 4 to the Act and section 7 of the 2003 Act.
[65] For more information on the Growth Duty and how this has been assessed, see the Combined Impact Assessment.

making, and we place a significant weight on the severity of harm when assessing the impacts of our measures.

A1.76 We have internal research functions, outlined in our Online Safety Research Agenda, to work with academic experts to broaden our evidence base.[66]

Enforcement

A1.77 Stakeholders said the success of measures depends on the ability to enforce measures proportionately.[67]

A1.78 Yoti suggested that visible investigations into noncompliance should be prioritised to show that inaction is unacceptable.[68]

Our response

A1.79 We have a variety of tools and methods to ensure compliance with the Act. Our supervision team has established relationships with the largest and riskiest services to ensure they understand the expectation of measures and can come into compliance quickly. We have broad powers to compel service providers to give us the information we need to carry out our functions.

A1.80 We have the powers to take enforcement action where we become aware of instances of noncompliance. We make decisions about whether to open enforcement investigations on a case-by-case basis. Since these powers came into force, we have acted swiftly to launch investigations into over 100 services, as well as using a range of other tools at our disposal to drive compliance. The opening and outcomes of our investigations are published on our website.

A1.81 Where we find a service provider has contravened its duties, we have the power to impose a penalty of up to 10% of qualifying worldwide revenue or £18 million (whichever is greater) and require remedial action. To date, we have issued fines to 11 service providers for noncompliance. In exceptional cases of continued noncompliance, where there is a significant level of risk of harm to users, we may apply to the court for an order that requires third parties to either restrict the supply of services to the service provider (such as advertising or payment services) or restricting access to the service itself for UK users.[69]

Service provider self-assessment

A1.82 Stakeholders said it was not in providers' interest to be transparent in self-assessments and asked whether Ofcom would police the self-assessment process.[70]

Our response

A1.83 The Act requires service providers to carry out a "suitable and sufficient" assessment of their risk of illegal harms and we have a range of powers to enforce that duty including, where relevant, a power to issue a decision which means the safety duties apply as if the provider concerned had identified a risk.[71]

---

[66] Ofcom (2024), Online Safety Research Agenda.
[67] Scottish Government response to the June 2025 Consultation, p.4; Yoti response to the June 2025 Consultation, p.22.
[68] Yoti response to the June 2025 Consultation, p.22.
[69] Ofcom (2024), Online Safety Enforcement Guidance.
[70] [✂]; NPCC response to the June 2025 Consultation, p.6.
[71] Section 134 of the 2023 Act.

'Safe harbour'

A1.84 Civil society stakeholders criticised the concept of 'safe harbour', saying that this meant services providers could be shielded from enforcement while users are still exposed to risks.[72] SWGfL recommended that 'safe harbour' should be removed or reformed in light of technical feasibility provisions.[73]

Our response

A1.85 The Act provides that compliance with the Codes is deemed compliance with the safety duties. We have no power to change the Act – any changes would be a matter for Government and Parliament.

Collaboration

A1.86 Stakeholders raised the importance of collaboration across a number of groups.

a) Stakeholders from civil society and public bodies noted the importance of cross-service provider collaboration to prevent harm and repeat offences by users.[74]
b) Yoti said international alignment should be strengthened through mechanisms like the Global Online Safety Regulators Network (GOSRN) to ensure consistent expectations for global service providers.[75]
c) Civil society stakeholders noted the importance of co-design of measures, public and academic engagement on our work.[76]

Our response

A1.87 We agree with stakeholders that collaboration can bring benefits. This includes engagement across sectors and expertise.

A1.88 Ofcom only has powers over regulated entities and can only regulate each service provider individually. There are practical challenges: we estimate that the sector comprises 100,000 services (and likely significantly more) based all over the world.

A1.89 We note the requirement to ensure service providers are fully compliant with ICO data protection requirements. While we encourage cross-service collaboration, this must be done in a way that adheres to data protection laws.

A1.90 Ofcom is involved in several international regulatory networks designed to enhance online safety protection globally. Notably, we co-founded GOSRN, a dedicated coordination forum for independent online safety regulators around the world who publish annual reports of progress.[77] GOSRN is the only global space dedicated exclusively to coordination among

---

[72] Antisemitism Policy Trust response to the June 2025 Consultation, p.5; FCA UK response to the June 2025 Consultation, p.2; Molly Rose Foundation response to the June 2025 Consultation, pp.1-2.
[73] SWGfL response to the June 2025 Consultation, p.2.
[74] Commissioner Designate for Victims of Crime in Northern Ireland response to the June 2025 Consultation, p.7; Domestic Abuse Commissioner response to the June 2025 Consultation, p.6; Internet Watch Foundation (IWF) response to the June 2025 Consultation, p.44; Marie Collins Foundation response to the June 2025 Consultation, p.9; Online Safety Network response to the June 2025 Consultation, p.23; UCL Gender and Tech Research Lab (IET) response to the June 2025 Consultation, p.3.
[75] Yoti response to the June 2025 Consultation, pp.22-23.
[76] Marie Collins Foundation response to the June 2025 Consultation, pp.5-6; UCL Gender and Tech Research Lab (IET) response to the June 2025 Consultation, p.5; VoiceBox response to the April 2025 User Controls Consultation, pp.4-5.
[77] Global Online Safety Regulators Network, 2025. Global Online Safety Regulators Network – Annual report 2025.

regulators on online safety. Where appropriate, the network aims to enhance coherence and coordination amongst international regulators, by providing a space for them to share insights, experience, and best practice.

A1.91 The GOSRN regulatory index compares international approach and perspectives to online safety regulation to aid in international collaboration of regulators.[78] The regulatory index is designed to further support regulators' activities towards regulatory coherence, as first outlined in the network's position statement on regulatory coherence and coordination in 2024. GOSRN has also published a three-year strategy outlining five priorities. These include building regulatory coherence across jurisdictions and facilitating the sharing of information and coordination to promote compliance.

A1.92 We recognise the value in hearing the voices of those with lived experience and the important role that these personal experiences can have in informing our approach to implementing the Act.

A1.93 Ofcom has a Lived Experience Team that seeks to incorporate the voices of adults and children with direct experience of online harm, including survivors and victims of specific harms, into our online safety work. These perspectives are used to inform our policymaking and monitor and evaluate the impact of our work to date.

Collaboration with law enforcement

A1.94 Law enforcement organisations and an individual stakeholder noted the importance of collaboration between service providers and law enforcement.[79] This included the importance of evidential chains for content depicting crimes, having fixed points of contact within service providers, and the quick removal of content depicting crimes online to respect victim's dignity.

Our response

A1.95 We recognise that the removal of content and accounts linked to illegal harms carries a risk of inadvertently destroying potential evidence for law enforcement. However, service providers are required to take proportionate steps to remove illegal content of which they become aware, and the Act does not give us powers to require providers to preserve evidence for the purposes of criminal enforcement.[80] The decision to retain data is a matter for the service provider. We do not consider that the risk that evidence may be lost is a reason not to recommend a measure which will reduce the overall illegal activity and protect users.

A1.96 It is outside the scope of our regulatory duties to enforce fixed points of contact or the manner in which evidential chains are managed.

Protection from primary priority content, priority content, and non-designated content

A1.97 The Molly Rose Foundation said we applied uneven protections to content that is harmful to children, with greater protections in place for primary priority suicide and self-harm content than for priority and non-designated content (such as depression content). It

[78] Global Online Safety Regulators Network, 2025. Regulatory Index: Comparing international approaches and perspectives to online safety regulation.
[79] [✂]; NPCC response to the June 2025 Consultation, p.2; Police Service of Northern Ireland response to the June 2025 Consultation, pp.1-2.
[80] Section 10(3)(b) of the 2023 Act.

noted that the interactions of these harms, and how they contribute towards cumulative harms, is well established.[81]

Our response

A1.98 Our Protection of Children Code reflects the different requirements set out by the Act for the types of content harmful to children. The Act requires that providers take proportionate steps to prevent children from encountering primary priority content, and to protect children from encountering priority and non-designated content. Our measures reflect these different duties so that the strongest safeguards are put in place where the harm is most severe and the benefits to children are the greatest.

A1.99 In our October 2026 statutory report on content harmful to children, we recommended that it is appropriate to add body stigma content and depression content, currently identified by Ofcom as kinds of non-designated content, to the category of priority content that is harmful to children. We consider that the evidence is now sufficiently established to justify the designation of body stigma and depression content as priority content, putting them on the same statutory footing as other kinds of priority content and ensuring that all service providers take appropriate steps to protect children from this kind of content. If the Secretary of State decides to add body stigma content and depression content to the Act as kinds of priority content, Ofcom will amend the relevant regulatory documents and guidance to reflect those changes.

A1.100 The Protection of Children Code recommends measures that specifically aim to mitigate the risk of cumulative harms for primary priority content, priority content and non-designated content – for example, our measures on recommender systems.[82]

Online safety of women and girls

A1.101 Civil society stakeholders raised the importance of measures to protect women and girls online, including protections for 16-18 year olds.[83] The Domestic Abuse Commissioner noted specific functionalities like friend suggestions, location features and gifting that may increase the risk of harm occurring on a service for victims of domestic abuse.[84] Glitch raised concerns about misogynoir content which can be lawful but harmful and recommended use of their Misogynoir Tracking tool.[85]

Our response

A1.102 The safety of women and girls is central to our online safety programme, and we are committed to driving meaningful change for women and girls across the UK. Our first iteration of the Illegal Content Codes created a strong foundation, and in November 2025 we published A Safer Life Online for Women and Girls: Practical Guidance for Tech Companies which is guidance on tackling violence against women and girls online.[86] We are currently working to encourage uptake of this guidance.

---

[81] Molly Rose Foundation response to the June 2025 Consultation, p.3.
[82] Protection of Children Codes of Practice for user-to-user services (Protection of Children Codes), Measures PCU E1 and PCU E2.
[83] Domestic Abuse Commissioner response to the June 2025 Consultation, p.5; UCL Gender and Tech Research Lab response to the June 2025 Consultation, p.3.
[84] Domestic Abuse Commissioner response to the June 2025 Consultation, pp.3-4.
[85] Glitch response to the June 2025 Consultation, pp.8, 16.
[86] Ofcom (2025), A Safer Life Online for Women and Girls: Practical Guidance for Tech Companies.

A1.103 The June 2025 Consultation included a dedicated measure on hash matching for intimate image abuse, which we confirmed in our May 2026 Statement on Intimate image abuse in recognition of the urgent need for better online protections for women and girls.

Evidence of child sexual exploitation and abuse (CSEA) harms

A1.104 The NPCC said the proposed measures marked a critical point in the UK's response to online harms, noting law enforcement faces unprecedented demand from CSEA referrals and the regulatory framework must reflect the scale, complexity, and urgency of this threat.[87] It said national data showed a sustained rise in CSEA offences, with 33,532 cases in the first quarter of 2025 (up 11% year-on-year) and 33,264 in the second quarter of 2025, with 45% involving an online element. It also noted sextortion offences reached 1,490 in the second quarter of 2025, mostly affecting boys aged 12 to 15. It said that these figures highlighted both increased reporting and the limits of current safeguards, stressing the need for enforceable standards.

Our response

A1.105 This response highlights the scale and severity of the harm and the necessity for a broad approach to tackling CSEA, including proactive technology/automated content moderation measures.

A1.106 We consider that our livestreaming measure, amendments to our CSAM hash matching measure and the proactive technology measure to address unknown CSAM represent a significant step forward in tackling CSEA. In particular, we perceive our proactive technology measure will help improve detection of previously unknown image-based CSAM, including material arising from financially motivated sexual extortion, enabling providers to act. Our amendments to the Illegal Content Judgement Guidance further strengthen this work.

Fraud

A1.107 Several stakeholders provided general evidence on fraud harms, the importance of addressing fraud harms to protect users, and their own work to tackle fraud.[88]

A1.108 Two stakeholders provided evidence in relation to fraudulent advertising as part of their evidence on fraud harms.[89]

A1.109 The Association of British Insurers (ABI) called for other parties to take further steps to address fraud.[90] It agreed with the Home Affairs Committee's recommendation that the Home Office should review progress of the implementation of the Online Fraud Charter and require services failing to implement measures to do so.[91]

[87] NPCC letter response to the June 2025 Consultation, p.1.
[88] Advertising Standards Authority (ASA) response to the June 2025 Consultation, p.6; Association of British Insurers (ABI) response to the June 2025 Consultation, pp.2,4; Financial Conduct Authority (FCA) response to the June 2025 Consultation, p.6; UK Finance response to the June 2025 Consultation, pp.2,13-14.
[89] ASA response to the June 2025 Consultation, p.6.; [✂].
[90] ABI response to the June 2025 Consultation, p.4.
[91] UK Government, 2023. Online Fraud Charter. Online Fraud Charter 2023 (accessible) – GOV.UK.

Our response

A1.110 We thank respondents for sharing this evidence and contributing to our evidence base on fraud harms, which will help to inform our future policy development work. We recognise stakeholder calls for further action by service providers and Ofcom to tackle fraud.

A1.111 This statement builds on the protections introduced in our December 2024 Statement on Protecting People from Illegal Harms, including through user sanctions measures that require providers to address fraud-related harms on their services. It also complements our wider work on online fraud, including our consultation on the draft Fraudulent Advertising Code of Practice, which proposed measures for Category 1 and Category 2A services to comply with the Act's fraudulent advertising duties. We expect to publish our decision on this in 2027.

A1.112 We note that there is overlap between some of the duties under the Act and the actions set out in the Online Fraud Charter.

Clarification of animal cruelty offences

A1.113 The Social Media Animal Cruelty Coalition (SMACC) said Ofcom should provide clearer and more comprehensive guidance to service providers on the full spectrum of animal-cruelty offences and harmful behaviours that may appear online, including those not explicitly designated as priority offences.[92]

Our response

A1.114 Ofcom does not have the power under the Act to treat content which is not illegal as if it was illegal, or to treat offences which are not priority offences as if they were priority offences.

A1.115 We note SMACC's response and recognise that animal-cruelty content can extend beyond material that meets the definition of priority illegal content, while still posing significant risks to users, particularly children.

A1.116 As set out in the April 2025 Statement, we have previously provided guidance on violent content that is harmful to children, including material that "depicts real or realistic violence against an animal or fictional creature, or the serious injury of an animal or fictional creature in graphic detail".[93] The examples in our April 2025 Statement are not exhaustive and we note that the examples raised by SMACC might constitute animal cruelty related harmful content.[94]

A1.117 We have also now included animal cruelty as a kind of illegal harm in-scope of the livestreaming measure, as explained in chapter 2: Livestreaming – Measure on reporting mechanism for imminent physical harm.

[92] Social Media Animal Cruelty Coalition (SMACC) response to the June 2025 Consultation, pp.16-18.
[93] Ofcom (2025), April 2025 Statement, Protecting Children from Harms Online.
[94] Ofcom (2025), April 2025 Statement, Protecting Children from Harms Online, Guidance on Content Harmful to Children, p.58.

Proposals for new measures

A1.118 A range of stakeholders proposed new measures in a variety of areas, including for us to include a range of additional measures within our Codes in relation to fraud harms.[95] [96]

Our response

A1.119 Suggestions to extend proposed measures are considered in the relevant chapter.

A1.120 We will consider whether any future legislative changes require updates to our current position and will consult before making any such changes as appropriate. However, we would like to thank the large number of stakeholders who took time to offer feedback to the June 2025 Consultation and provide these suggestions, which we will factor into any future work.

[95] New measures were suggested across the following areas: safety standards, transparency, and governance, age assurance, identity verification and user controls, further proactive technologies, measures to address emerging risks like AI, monetisation, and immersive environments, support for content moderation, redress and support for victims and survivors, support for law enforcement, standardisation of reporting channels, safeguards for specific harms, measures aimed to tackling violence against women and girls, technical feasibility, increasing oversight and transparency for fraud, hash matching and user tools to report fraud and action on fraudulent advertising.

[96] A member of the Philippine Survivor Network response to the June 2025 Consultation, p.17; BILETA response to the June 2025 Consultation, p.2, 42; Center for Countering Digital Harm (CCDH) response to the June 2025 Consultation, p.1; CETATEA VIITORULUI response to the June 2025 Consultation, p.2; Check my Ads Institute response to the June 2025 Consultation, pp.14, 15; Commissioner Designate for Victims of Crime for Northern Ireland response to the June 2025 Consultation, p.5; Domestic Abuse Commissioner response to the June 2025 Consultation, pp.2, 3, 5-7; Glitch response to the June 2025 Consultation, pp.3, 7-9, 12; [✂]; Institute for Engineering and Technology response to the June 2025 Consultation, p.1; International Justice Mission response to the June 2025 Consultation, pp.16, 17; IWF response to the June 2025 Consultation, pp.35, 36, 37, 38, 39-41; Jones, C response to the June 2025 Consultation, p.1; Lucy Faithfull Foundation response to the June 2025 Consultation, pp.3, 4, 5, 6, 7; Molly Rose Foundation response to the June 2025 Consultation, p.4; [✂]; NPCC response to the June 2025 Consultation, pp.1, 2, 14; NSPCC response to the June 2025 Consultation, pp.46, 47; PSNI response to the June 2025 Consultation, p.2; Scottish Government response to the June 2025 Consultation, p.4; Social Media Animal Cruelty Coalition response to the June 2025 Consultation, p.8; Together Declaration Campaign response to the June 2025 Consultation, p.6; [✂]; UCL Gender and Tech Research Lab response to the June 2025 Consultation, pp. 1, 2; UK Finance response to the June 2025 Consultation, p.11; Yoti response to the June 2025 Consultation, p.23.

A2. Livestreaming

Further stakeholder responses received on the proposals in general by theme

Evidence request

A2.1 The Molly Rose Foundation said it was dismayed that we had asked civil society for more evidence to justify stronger action, despite acknowledging that some services already go further to protect users. It noted that we had not used our own disclosure powers to assess the effectiveness of these measures.[97]

Our response

A2.2 We have used a range of evidence sources to inform our measures including from meetings with stakeholder and requests for information (RFIs) on existing practice to inform these measures. We consider it is useful to ask stakeholders to provide additional evidence as part of a consultation process to ensure we can make well-informed decisions.

Limitations of the measures

A2.3 Several stakeholders raised concerns about the limitations of the proposed reporting and content moderation measures for livestreaming to protect all users. These included concerns that there is no minimum standard for implementation of the effectiveness of the measure, that the measures are technically insufficient and that the scope of the measures were "drawn too narrowly".[98]

Our response

A2.4 We recognise concerns raised however we consider that the approach set out in consultation is proportionate. The proposed measures would operate alongside wider illegal content duties which already recommend services to assess effectiveness and take action where mitigations are not working.

Circumvention methods

A2.5 The Antisemitism Policy Trust felt that the proposals do not eliminate the weakest links in the process, including the speed of the process and the use of virtual private network (VPN)/geocircumvention, allowing some illegal content to still be livestreamed for a dangerous interval before being removed.[99] The Canadian Centre for Child Protection (C3P) also felt we should give consideration of how users access a service via a terms of reference or a VPN and how these impact the level of risk.[100]

[97] Molly Rose Foundation response to the June 2025 Additional Safety Measures Consultation (June 2025 Consultation), p.11.
[98] 5Rights response to the June 2025 Consultation, pp.2, 4; Children's Commissioner's Office (CCO) response to the June 2025 Consultation, p.5; South West Grid for Learning (SWGfL) response to the June 2025 Consultation, p.8.
[99] Antisemitism Policy Trust response to the June 2025 Consultation, p.1.
[100] Canadian Centre for Child Protection (C3P) response to the June 2025 Consultation, p.8.

Our response

A2.6 We accept the likelihood that even where services do deploy safety measures, some illegal content will still be livestreamed for a period of time before being removed. As highlighted in our June 2025 Additional Safety Measures Consultation (June 2025 Consultation), the real-time nature of livestreaming makes content moderation difficult, even with automated tools. However, our existing measures already help mitigate this risk by requiring user reporting features that are easy to find, access and use; that providers prioritise content awaiting moderation; and that content moderation functions should be appropriately resourced thus providing tools to allow removal as quickly as possible to give effect to its internal content policies and performance targets.[101] Our additional reporting measure goes further to allow easy reporting of content where there is an imminent risk of physical harm.

A2.7 We note stakeholders' concerns about VPNs. We discuss our approach to VPNs in the introductory chapter of annex 1: Further stakeholder responses.

Messaging services and Com groups

A2.8 The Molly Rose Foundation expressed concern about our limited powers to address risks from private messaging services, which offer similar functionalities and risks as livestreams and that large group calls could allow harms to migrate from livestreaming to other features.[102] It said our proposals had misunderstood the threat from Com groups, where victims are coerced into interconnected harms like suicide and self-harm. It mentioned that it had raised the issues of Com groups in previous responses. It noted that these groups pose specific risks, grooming victims into self-harm, producing child sexual abuse material (CSAM) and other linked offences, and that livestreaming is central to this threat.[103] It also said that measures to reduce livestreaming risks only acted when users were already live or facing imminent physical harm, whereas Com groups groom children via messaging and then coerce them on livestreams. It felt that more friction should prevent victims starting a livestream.[104]

Our response

A2.9 We understand the Molly Rose Foundation's concerns about where harmful livestreaming content can migrate to other features such as private messaging services or large group chats and acknowledge our limited powers in these areas. However, measure ICU F1.4 (Safety defaults – direct messaging) mitigates some of the risks messaging services present to children. It sets out that if a service has direct messaging functionality, the provider should implement default settings ensuring that:

a) Where the service has user connection functionality, child user accounts can only receive direct messages from user accounts with which they have a specified connection; and
b) If the service does not have user connection functionality, users operating a child user account are provided with a means of actively confirming whether to receive a direct message sent from another user account before it is visible to them.

---

[101] It should be noted that the content moderation measures are segmented to large/multi-risk services only. Other services in scope of this measure may not be within scope of the contend moderation measures.
[102] Molly Rose Foundation response to the June 2025 Consultation, pp.11-13.
[103] Molly Rose Foundation response to the June 2025 Consultation, p.4.
[104] Molly Rose Foundation response to the June 2025 Consultation, pp.10-11.

A2.10 We have identified cross-platform and cross-harm risks, including risks arising from messaging, in our Illegal Harms and Children's Register of Risks. These recognise that children commonly use multiple services and take part in group chats, where harmful content may be shared and service functionalities can combine to create pathways to harm. Providers should therefore reflect these factors in their risk assessments and risk profiles.

Measures applying to livestreamed content uploaded post broadcast

A2.11 Barnardo's asked us to clarify how these protections would apply to livestreamed content that is uploaded after broadcast, particularly in relation to moderating interactions within comments.[105]

Our response

A2.12 These measures were intended to apply to content that was broadcast in real time via a livestream. Once a livestream has ended and the content is later uploaded or retained on a service, it would no longer fall within the scope of the proposed livestreaming measure. However, where livestreamed content (including interaction in comments) is made available after broadcast the relevant measures set out in the Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes) and Protection of Children Code of Practice for user-to-user services (Protection of Children Code) would apply, including recommendation relating to content moderation and the management of illegal content on a service.

Impact on creators

A2.13 Name Withheld 9 said that creators who make a livelihood from creating livestreams could face financial impact if their content is removed as a result of these measures.[106]

Our response

A2.14 We recognise that reporting tools may be misused, including to make malicious reports or to report non-imminent content to secure a preferred outcome. Services should have mechanisms under the Illegal Content Codes to address manifestly unfounded reports (ICU D13 – Exception: manifestly unfounded complaints).

A2.15 However, we acknowledge that incorrect content removal could affect creators, and we expect services to apply informed moderation practices to reduce the likelihood of such outcomes.

Livestreaming within the island of Ireland

A2.16 The Advisory Committee for Northern Ireland highlighted Northern Ireland's land border and said services should address issues where accounts registered abroad livestream harmful content affecting Northern Ireland. It recommended we work with services and Irish regulators to ensure such content can be blocked or removed and prevent loopholes.[107]

---

[105] Barnardo's response to the June 2025 Consultation, p.3.
[106] Name Withheld 9 response to the June 2025 Consultation, p.2.
[107] Advisory Committee for Northern Ireland response to the June 2025 Consultation, p.5.

Our response

A2.17 We recognise the concern that livestreamed harmful content affecting users in Northern Ireland may originate from accounts registered or operated outside Northern Ireland or the UK. The Online Safety Act 2023 (the Act) applies to services based on their accessibility to, and impact on, UK users rather than the location of an account or where content is streamed from. We therefore expect providers to address risks to users in Northern Ireland in the same way as risks to users elsewhere in the UK, including where those risks arise cross-border.

A2.18 We continue to use our bilateral partnerships with key counterpart online safety regulators, including Ireland's Coimisiún na Meán, to help drive better safety outcomes for UK users of services increasingly provided by global digital companies. We are contributing to regional and international processes that seek to develop norms and standards for online safety and user protection.

Support for application of measures to end-to-end-encryption services

A2.19 International Justice Mission said that the measures, relating to livestreaming should apply to end-to-end-encryption services.[108]

A2.20 The Internet Watch Foundation (IWF) supported extending the measures to all types of livestreamed broadcasts; it noted that Discord's Go Live feature would adopt end-to-end-encryption in March 2026 for many-to-many broadcasts.[109] IWF also asked for clarity of how moderators can intervene in end-to-end-encryption livestreams.[110]

Our response

A2.21 We noted there is mixed feedback on how measures should apply in these environments but note that all services need to adhere to the duties in the Act. The Act states that Ofcom must have regard to the principle that the measures in our Codes must be proportionate and technically feasible. As such, although the measure under discussion applies to providers of all user-to-user services, the text of the recommendation itself makes clear that we do not expect services to take down content where it is not currently technically feasible for them to achieve this outcome.[111]

A2.22 We recommend that providers of all user-to-user services should, as part of its content moderation function, have systems and processed designed to swiftly take down illegal content and/or illegal content proxy of which it is aware, unless it is currently not technically feasible for them to achieve this outcome (ICU C2).

Risk based approach to applying measures

A2.23 5Rights Foundation reiterated its feedback to the draft Illegal Content Codes that linking risks to specific offences discouraged services from understanding how their systems and features cause harm.[112]

---

[108] International Justice Mission response to the June 2025 Consultation, p.4.
[109] Internet Watch Foundation (IWF) response to the June 2025 Consultation, p.5.
[110] IWF response to the June 2025 Consultation, p.6.
[111] Privacy and Electronic Communications (EC Directive) Regulations, 2003.
[112] 5Rights Foundation response to the June 2025 Consultation, p.5;

A2.24 Francis, S. argued that designating services as medium or high risk for terrorism, hate or harassment is vague and risked over-censorship.[113]

Our response

A2.25 The Act requires services to conduct an illegal content risk assessment to identify the kinds of illegal content that are present. We use these risk levels to ensure our measures are proportionate to the size and capacity of services as well as the potential of harm to users and other individuals.

Further stakeholder responses received on our measure on reporting for imminent harm by theme

Interaction with existing measures and legislation

A2.26 Two industry stakeholders said that the measure unnecessarily duplicated our existing reporting and complaints measures. X said that the measure could add complexity, reduce accessibility and slow review times, while Meta Platforms Inc. (Meta) argued the measure would create a disproportionate risk of over-removal relative to its benefits.[114]

A2.27 A further two respondents raised the interaction of this measure with some service's obligations under European Union (EU) law including to notify law enforcement agencies of suspicions of a criminal offence involving threat to the life or safety of a person (Article 18 Digital Services Act (DSA)) and terrorist content involving imminent threat to life (Article 14 Terrorist Content Online (TCO).[115]

Our response

A2.28 We consider that given the risks associated with livestreaming as set out in our June 2025 Consultation and the associated challenges for moderation, a specific category for this type of content is not duplicative but builds on existing reporting and complaints measures. It will enable services to be alerted with specific and real time signposts to suspected illegal content containing imminent physical harm. This will allow services to take appropriate action.

A2.29 In terms of existing legislation, these measures are designed to alert services of the existence of livestreams that depict an imminent risk of physical harm and take appropriate moderation decisions. These measures do not duplicate the notification requirements in Article 14 TSO or Article 18 DSA.

A2.30 Where services are required under the DSA or other legislation to submit transparency reports with fixed reporting categories, they should be able to categorise any moderation decision to the appropriate reporting category. How the user reporting category links with transparency reporting categories is a decision for services.

Existing practice and flexibility of measure

A2.31 Some stakeholders noted that services already have in place categories that enable users to report instances of imminent physical harm, however these did not use the term

[113] Francis, S. response to the June 2025 Consultation, p.4.
[114] Meta Platforms Inc. (Meta) response to the June 2025 Consultation, pp.5-7; X response to the June 2025 Consultation, p.1.
[115] [✂]; [✂].

"imminent physical harm". They argued that the existing categories serve the same function as this measure.[116]

A2.32 In addition, Google LLC. and the UK Association for Interactive Entertainment (Ukie) called for flexibility in the implementation of the measure, stating that the design of choice categories and reporting mechanisms should be up to the provider. Ukie also asked us to consult industry before finalising categories to ensure language and functionality match user experience.[117]

A2.33 [✂].[118]

Our response

A2.34 Measure ICU D17 has flexibility for providers to design the reporting categories as works for them. Providers can use alternative wording if it meets the aim of allowing users to show that the livestream contains content depicting imminent physical harm in an appropriate manner.

A2.35 In both our June 2025 Consultation, and in paragraph 2.46 of chapter 2: Livestreaming, we set out what types of categories would not comply with this measure because the categories are not specific to the risk of imminent physical harm.

A2.36 We have also said that if a service already has a category that allows user to report that the livestream shows imminent physical harm, the service may already comply with this measure.

A2.37 We therefore consider that there is enough flexibility built into the measure for different services with different interfaces to adapt the measure if it achieves the same outcomes.

Use of the term "imminent physical harm"

A2.38 In its response, Meta said that the use of the term "imminent physical harm" would not result in any additional illegal content being reported to services.[119] Meta also said that the proposed measure would enable users to report content that was not illegal and would not lead to a reduction of harm online.[120]

Our response

A2.39 The aim of the measure is not to increase reporting but to allow for targeted reporting of livestreams containing the harms in scope.

A2.40 However, we understand that reporting measures may create instances where services receive reports which may include non-illegal content. We acknowledge that it is a possibility that in some narrow circumstances, the reporting measure may lead to reports of non-illegal content.

A2.41 We consider that "imminent physical harm" or equivalent term that a service can choose, can act as a proxy for certain kinds of illegal harm (such as terror, illegal suicide content). This term is easy to understand for users who wish to report this type of content rather

---

[116] [✂]; [✂]; [✂]; [✂].
[117] Google LLC. response to the June 2025 Consultation, pp.8-9; Ukie response to the June 2025 Consultation, pp.11-13.
[118] [✂].
[119] Meta response to the June 2025 Consultation, pp.5-6.
[120] Meta response to the June 2025 Consultation, pp.5-6.

than using terms like “terror” which may not be easy for a user to determine in the moment.

Suggestions to increase the effectiveness of the measure

A2.42 We received responses stating that this measure would be more effective if services put in place actions such as alerting users on the outcome of their report, providing support to users – particularly victims of child sexual exploitation and abuse (CSEA) or those displaying behaviours relating to suicide or self-harm – and providing an option for open-text when users use the “imminent physical harm” button.[121]

Our response

A2.43 While we consider that additional actions may be useful, we have not amended the measure to include this. The action taken after the report sits with our content moderation measures. Within these, we have a measure (ICU D4/ICS D3) that applies to certain services which recommends providers should acknowledge receipt of a complaint and provide complainants with an indicative timeframe for when a complaint might be resolved.[122]

A2.44 We also have a measure (ICU D5/ICS D4) which recommends certain services should inform a complainant about the possible outcomes of a complaint, including whether the service will update the complainant on the outcome. [123]

A2.45 As mentioned in chapter 2: Livestreaming, paragraph 2.47, providers have the flexibility to design this reporting function for this measure in a way that best suits their service, and they may wish to offer additional actions such as an open-text option for gathering more data. Services may already offer some of these actions as part of their existing duties under the Illegal Content and Protection of Children Codes.

Other offences involving physical harm

A2.46 5Rights Foundation and the Online Safety Network (OS Network) raised concerns that the scope of the measure excluded some illegal harms that are present in our Illegal Harms Register of Risks (Illegal Harms Register), such as extreme pornography and human trafficking.[124]

Our response

A2.47 We have included the key priority offences relating to livestreaming and imminent physical harm in the scope of this measure as detailed in our Risk Profiles for livestreaming. We

[121] A member of the Philippine Survivor Network response to the June 2025 Consultation, pp.5-6; BILETA response to the June 2025 Consultation, p.5; C3P response to the June 2025 Consultation, pp.5-6; Internet Matters response to the June 2025 Consultation, pp.4-6; IWF response to the June 2025 Consultation, pp.8-9; Refuge response to the June 2025 Consultation, p.4; Samaritans response to the June 2025 Consultation, pp.2-3; SWGfL response to the June 2025 Consultation, p.9; [✂].

[122] Illegal Content Codes of Practice for user-to-user services, Measure ICU D4 applies to large user-to-user services; user-to-user services at medium or high risk of any kind of illegal harm. Illegal Content Codes of Practice for search services, Measure ICS D3 applies to providers of large general search services; providers of services at medium or high risk of any kind of illegal harm.

[123] Illegal Content Codes of Practice for user-to-user services, Measure ICU D5 applies to providers of large user-to-user services likely to be accessed by children; providers of services at medium or high risk of any kind of illegal harm, which are likely to be accessed by children; Illegal Content Codes of Practice for search services, Measure ICS D4 applies to providers of large general search services likely to be accessed by children; providers of services at medium or high risk of any kind of illegal harm.

[124] 5Rights Foundation response to the June 2025 Consultation, p.4; Online Safety Network (OS Network) response to the June 2025 Consultation, p.5.

consider these to be the illegal harms most strongly linked to livestreaming. While illegal content relating to extreme pornography or human trafficking may be connected to functionalities like livestreaming, the Illegal Harms Register currently presents less evidence for these harms.

A2.48 We also consider that there may be significant overlaps in the occurrence of harms included in the scope of this measure, such as terrorism or CSEA content, and other illegal harms that are outside of the Risk Profiles. Services with risk of harms not directly included in our scope are still likely to implement this measure.

Accessible and effective reporting

A2.49 Internet Matters, 5Rights Foundation, the Children's Commissioner's Office (CCO), the Welsh Government (Digital Resilience in Education), and C3P cited barriers to children reporting including lack of trust and complexity of design.[125] 5Rights Foundation also cited research which showed children had mixed views on effectiveness, including our own research which found children did not have confidence in reporting systems including what happened after.[126]

A2.50 These stakeholders recommended that reporting tools needed to be quick and easy to find, use simple processes and language, and be age-appropriate. They regarded design as critical and should include safety considerations to gain the trust of children along with language considerations. Clear signposting and expected response times should also be used. However, Internet Matters also recognised that reporting and complaints provisions in the Protection of Children Code could apply to livestreaming.[127]

A2.51 [✂] and a member of the Philippine Survivor Network also highlighted the need for reporting tools to be simple, quick to use and accessible for all users, not just children while also being intuitive for all ages with differing levels of digital maturity.[128] A member of the Philippine Survivor Network also considered that categories should be specific enough to identify issues with a visible button during livestreaming.[129]

A2.52 The Internet Justice Mission highlighted the need for trained moderators, AI triage, and language support.[130]

A2.53 The CCO recommended that children should be consulted on systems.[131]

Our response

A2.54 We recognise that children can find reporting and complaints systems difficult to access and understand as such systems are often designed for adults. Therefore, the Illegal Content and Protection of Children Codes already set out reporting/complaints and content moderation measures which should address the issues raised by stakeholders.

---

[125] 5Rights Foundation response to the June 2025 Consultation, p.8; C3P response to the June 2025 Consultation, pp.6-7; CCO response to the June 2025 Consultation, p.7; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.5; Internet Matters response to the June 2025 Consultation, pp.4-5; International Justice Mission response to the June 2025 Consultation, p.9.
[126] 5Rights Foundation response to the June 2025 Consultation, p.8.
[127] Internet Matters response to the June 2025 Consultation, p.5.
[128] A member of the Philippine Survivor Network response to the June 2025 Consultation, p.5; [✂].
[129] A member of the Philippine Survivor Network response to the June 2025 Consultation, p.5.
[130] International Justice Mission response to the June 2025 Consultation, p9.
[131] CCO response to the June 2025 Consultation, pp.4-5.

- Reporting and complaints: systems must be accessible for children, including having easy to find, easy to access and easy to use complaints processes,[132] along with information on the processes and how the complaint will be handled along with providing time frames for resolution.[133]
- Content moderation: providers must implement systems and processes designed to review and assess content present on a child accessible part of the service that the provider has reason to suspect may be relevant content that is harmful to children.[134] Providers should also ensure individuals working in content moderation receive training and materials that enable them to fulfil their role in moderating content present on a child-accessible part of the service.[135]

A2.55 We allow services to have the flexibility to define their own categories to allow them to target these to their user base and risk assessments/profiles. This additional measure (ICU D17) specifies that providers must have a mechanism for reporting imminent physical harm.

Recommendations to improve accessibility

A2.56 Internet Matters stressed that providers should clearly communicate new reporting options to child users.[136]

A2.57 The National Police Chiefs' Council (NPCC), C3P, and the Evangelical Alliance UK called for reporting processes to be barrier-free, simple, clear, and prominent, using minimal steps and plain language such as "report immediate danger" or "imminent harm".[137]

A2.58 The NPCC also recommended a free text option and real time escalation to moderators/law enforcement.[138]

Our response

A2.59 The recommendation for service providers to implement easy to find, easy to access and easy to use complaints systems and processes that are designed so that they only include reasonably necessary steps are set out in the Illegal Content and Protection of Children Codes. The Codes also include recommendation to provide information prior to the submission of a complaint, provide indicative timeframes and information on how a complaint will be handled.

A2.60 We do not specify how providers should define imminent harms but allow them flexibility so they can most effectively target definitions of likely harms to their users according to their risk assessments/profiles and user base.

---

[132] Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes), Measure ICU D2; Protection of Children Codes for user-to-user services (Protection of Children Code), Measure PCU D2.
[133] Illegal Content Codes, Measures ICU D3-ICU D5; Protection of Children Codes: PCU D3-PCU D5.
[134] Protection of Children Codes, Measure PCU C1
[135] Protection of Children Code, Measure PCU C7.
[136] Internet Matters response to the June 2025 Consultation, p.5.
[137] C3P response to the June 2025 Consultation, p.6; Evangelical Alliance UK response to the June 2025 Consultation, p.3; National Police Chiefs' Council (NPCC) response to the June 2025 Consultation, p.3.
[138] NPCC response to the June 2025 Consultation, p.3.

Disagreement that only live acts of animal abuse amounts to animal cruelty offence

A2.61 The Social Media Animal Cruelty Coalition (SMACC) noted it disagreed that only live acts met the thresholds for encouraging, assisting, or conspiring to commit animal cruelty under the Act, stating recorded acts were the main contributors. It gave examples of how services are being used to post animal cruelty content and cited a Royal Society for the Prevention of Cruelty to Animals (RSPCA) prosecution involving TikTok videos as evidence that recorded content can meet the Act's test for encouraging or assisting animal cruelty.[139]

Our response

A2.62 We received similar responses to our August 2024 Further Consultation on Torture and Animal Cruelty. We responded to this in paragraphs 2.364 to 2.365 in the Illegal Content Judgement Guidance chapter in the December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement).[140]

Harms in scope: fraud

A2.63 UK Finance said that victims often did not recognise fraud promptly because it appeared legitimate and noted that emotional barriers like embarrassment or shame discouraged reporting, especially in public contexts like livestream gifting or influencer interactions. It recommended creating a dedicated fraud reporting category on gifting-enabled platforms to enable faster verification and classification.[141]

Our response

A2.64 The focus of this measure is on content that can cause imminent physical harm. It does not apply to harms like fraud where there is no such risk. However, our Illegal Content Codes contain other reporting and complaints measures that are relevant to fraud. These measures set out that services should have easy to find, easy to access and easy to use complaints systems and processes, and that large services that are at medium or high risk of fraud should have a dedicated reporting channel for trusted flaggers to report fraud.

Harms in scope: psychological harm

A2.65 Several stakeholders emphasised that harmful content could cause psychological harm to children and urged us to add psychological harm to the reporting measure.[142]

Our response

A2.66 The focus of this measure is on imminent physical harm.

A2.67 In the Protection of Children Code, we have measures in place that recommended service providers ensure they have systems and processes in place that enable users to report and complain about content that is harmful to children.

---

[139] Social Media Animal Cruelty Coalition (SMACC) response to the June 2025 Consultation, p.17.
[140] Ofcom (2024), December 2024 Statement, Protecting people from illegal harms online, volume 3, p.75.
[141] UK Finance response to the June 2025 Consultation, p.3.
[142] Barnardo's response to the June 2025 Consultation, p.2; Department of Justice for Northern Ireland response to the June 2025 Consultation, p.2; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.3.

Need for trained moderations/appeals process

A2.68 [✂].[143]

A2.69 [✂].[144]

Our response

A2.70 There are recommended measures ICU C7 (Provision of training and materials to individuals working in content moderation) in place for our Illegal Content Codes around training moderators which covers multi risk services. We would expect most services in scope of this livestreaming measure to be in scope of measure ICU C7.

A2.71 We have measures in place to appropriately deal with appeals. Under the Act, all services have a duty to operate a complaints procedure that allows for relevant kinds of complaints, including appeals, to be made. Appeals are an important protection for complainants' and users' rights to freedom of expression. Providers should also take appropriate steps to reverse the effects of an incorrect decision, otherwise successfully appealing does not help the complainant or user concerned.

Harms in scope: Inclusion of extreme violent, challenges and dangerous content

A2.72 The Molly Rose Foundation said the reasoning for not including serious offences like extreme violence was unclear.[145] 5Rights Foundation raised concerns about excluding harms that put children at risk of imminent physical harm such as challenges and dangerous stunts, noting the omission of this content from both measures, and citing a recent fatality during an extreme online challenge.[146]

Our response

A2.73 This reporting measure is focused on illegal harms, and we recognise that some extreme violent content may not amount to the priority illegal content included in this measure.

A2.74 We note 5Rights Foundation's concerns that the measure does not include harms that put children at risk of imminent harm. For our June 2025 Consultation, we decided to focus this measure on illegal harms. As we did not consult on including any primary priority content or priority content that is harmful to children in scope of this measure, we will not be adding this to our recommendations at this stage. However, if users do utilise this function for reporting of harms relating to protection of children we expect services to take relevant actions in relation to their Protection of Children duties.

Harms in scope: Harassment, stalking, threats, and abuse

A2.75 Refuge noted that we defined "imminent physical harm" as CSEA and threats to life, specifying scenarios including terrorist attacks, real-time child sexual abuse, suicide attempts, and incitement of violence. It supported these harms being in scope but argued the measure did not sufficiently cover the risks around gendered violence and livestreams,

[143] [✂].
[144] [✂].
[145] Molly Rose Foundation response to the June 2025 Consultation, p.12.
[146] 5Rights Foundation response to the June 2025 Consultation, p.5.

referencing End Violence Against Women's response to the consultation and cases of livestreamed murders and torture of women.[147]

A2.76 Further, Refuge noted the online harassment of women and girls was common, with risks of doxxing[148] on livestreams leading to harassment and abuse.[149] It questioned why this harm was not included in the reporting measure.

Our response

A2.77 We want to clarify that terrorism content, grooming or image-based CSAM, encouraging or assisting suicide and self-harm, hate, or harassment, stalking, threats and abuse and animal cruelty offences are included in the measure which means that providers which are medium or high risk of these offences should implement this measure.

A2.78 We recognise the concerns raised about the online harassment and abuse of women and girls, including harms facilitated through livestream functionality. These harms may amount to priority offences such as harassment, stalking, threats and abuse, and our existing measures recommend providers offer reporting and complaints mechanisms and to take appropriate action in response to reports. However, the measure considered here is narrower in scope and is specifically intended to support the rapid reporting of content indicating an imminent risk of physical harm.

Harms in scope: narrowing list of harms included

A2.79 Microsoft noted that we currently recommend the measure for certain user-to-user services at medium or high risk of content harms, including hate, harassment, and abuse. It suggested we consider narrowing the list of harms to categories most likely to cause imminent physical harm so reporting remains targeted and high risk reports can be prioritised and escalated.[150]

Our response

A2.80 As set out in our June 2025 Consultation, the livestreaming functionality often plays a significant role in disseminating content related to the harms included in this measure.

A2.81 Narrowing the list of harms which determines which services are in scope would also not improve the targeting of reports on a service. The action of reporting is done by the user who will apply their understanding of imminent physical harm. The list of harms ensures that the reporting category is present across the range of relevant livestreaming services so that users are able to report physical harm where it appears.

A2.82 In conclusion, based on the argument and evidence we have decided not to narrow the list of offences included in the measure.

Actions following identification of content – alerting authorities

A2.83 Stakeholders, including the NPCC, [✂], the Advisory Committee for Northern Ireland, and the OS Network, suggested that services should report instances of imminent physical

[147] Refuge response to the June 2025 Consultation, p.3.
[148] The intentional online exposure of an individual's identity, private information or personal details without their consent. eSafety Commissioner, 2020. What is doxing or doxxing?
[149] Refuge response to the June 2025 Consultation, p.4.
[150] Microsoft response to the June 2025 Consultation, p.2.

harms to authorities.[151] The Advisory Committee for Northern Ireland also suggested that the measure should include record-keeping elements so that authorities can use these as part of their investigations.[152] The NPCC stated that harmful material is reported to its Counter Terrorism unit by members of the public.[153]

Our response

A2.84 Our powers do not extend to these types of data sharing and recording elements. However, we are aware that some agreements are in place between services and authorities in terms of sharing information. These arrangements are between services and authorities and we are not involved.

A2.85 However, providers of regulated user-to-user services are required to report detected and unreported CSEA content to the designated reporting body housed in the National Crime Agency (NCA).[154] Providers may also have obligations to report CSEA content in other jurisdictions or may have voluntary arrangements in place. For example, US providers are obliged under US law to report to the National Center for Missing & Exploited Children (NCMEC) when they become aware of child sexual abuse on their services.

Actions following identification of content – compliance

A2.86 Stakeholders highlighted wider safety approaches that providers may take for livestreamed content, including the use of content moderation and/or safety by design features, such as account settings or parental controls, which protects users, particularly those aged under 18. The Marie Collins Foundation said that there was not sufficient clarity on the consequences of not complying with this measure.[155]

A2.87 The Molly Rose Foundation was concerned that providers could "game" this measure by stating that their existing reporting functions already comply.[156]

Our response

A2.88 Our approach to compliance of this measure will be in line with our approach to enforcement that we have in place with all our measures. We assess providers' compliance based on our Online Safety Enforcement Guidance.[157]

Limitations of measure – reactive nature of measure

A2.89 Some stakeholders, including the Marie Collins Foundatiom, the Lucy Faithfull Foundation, the Internet Watch Foundation (IWF), and the British and Irish Law Education and Technology Association (BILETA) said that Measure ICU D17 was not effective as it is reactive in nature, and the illegal content has already occurred online by the time users report. Some stated that we should focus on proactive measures that stops the harm

[151] Advisory Committee for Northern Ireland response to the June 2025 Consultation, p.2; NPCC response to the June 2025 Consultation, p.2; OS Network response to the June 2025 Consultation, p.6.
[152] Advisory Committee for Northern Ireland response to the June 2025 Consultation, p.4.
[153] NPCC confidential response to the June 2025 Consultation, p.2.
[154] Ofcom (2026), Duty to report child sexual exploitation and abuse (CSEA) content: know the rules and how to comply. Service providers are required to report detected CSEA to the NCA, where they do not already report to an equivalent foreign agency, such as the US National Center for Missing and Exploited Children (NCMEC). Note that for a non-UK provider of such a service, the obligation only extends to UK-linked CSEA content.
[155] Marie Collins Foundation response to the June 2025 Consultation, p.5.
[156] Molly Rose Foundation response to the June 2025 Consultation, p.13.
[157] Ofcom (2024), Online Safety Enforcement Guidance.

occurring online in the first instance.[158] The National Society for the Prevention of Cruelty to Children (NSPCC) made similar arguments and noted that children are reluctant to report.[159]

Our response

A2.90 We recognise the importance of reducing the risk of illegal harm occurring online. However, there will continue to be instances when illegal content manifests online and it is important that users can report when this happens so that services can be made aware as quickly as possible and take appropriate action.

Limitations of measure – burden on users

A2.91 The Marie Collins Foundation and C3P noted that this measure places the responsibility on users, including children, to take action. They argued that we should put in place measures that place the onus on providers to ensure that the harm does not occur on the service in the first instance.[160] C3P also highlighted that children can be fearful of reporting due to consequences from perpetrators.[161]

Our response

A2.92 We agree on the importance of ensuring that illegal harm does not occur online in the first instance. However, we consider it is important that if this type of illegal harm occurs online that users, including victims, have the ability to report it to providers. Our Illegal Content Codes of Practice contains measures on reporting and complaints that acknowledge that children are reluctant to report. These measures have the aim of encouraging children to report.[162]

Cross-platform coordination

A2.93 C3P said that providers should use consistent designs, categories, and language for reporting functions across services to allow a culture of understanding of harms and make reporting easier.[163]

Our response

A2.94 Recommendations around accessibility and design are set out in the Illegal Content and Protection of Children Codes. We set out basic principles, but they allow providers the flexibility to design accessible easy to use reporting systems according to their risk assessments/profiles and user base.

Support for users

A2.95 Samaritans called on services to support livestreamers and users following a report.[164]

---

[158] BILETA response to the June 2025 Consultation, p.13; IWF response to the June 2025 Consultation, p.6; Lucy Faithfull Foundation response to the June 2025 Consultation, p.3; Marie Collins Foundation response to the June 2025 Consultation, p.5.
[159] NSPCC response to the June 2025 Consultation, p.4.
[160] C3P response to the June 2025 Consultation, p.6; Marie Collins Foundation response to the June 2025 Consultation, p.5.
[161] C3P response to the June 2025 Consultation, p.7.
[162] Illegal Content Codes, Measures ICU D1-D14.
[163] C3P response to the June 2025 Consultation, p.6.
[164] Samaritans response to the June 2025 Consultation, pp.2-3.

Our response

A2.96 Although this is not an aspect of the measure, we did note in our June 2025 Consultation (paragraphs 7.6-7.7) that some providers already signpost users at risk of suicide to crisis prevention information. We encouraged providers in scope of this measure to signpost to crisis prevention information and to notify emergency services when livestreaming users are at risk of taking their life or harming themselves.

Recommendations for tools (various)

A2.97 There was a variety of other recommendations from stakeholders on further actions or detail that we should include as part of this measure. A member of the Philippine Survivor Network, recommended that services should provide guidance on the importance of reporting while Internet Matters said that children valued simple prompts.[165] Both South West Grid for Learning (SWGfL) and A member of the Philippine Survivor Network, said that services should provide the option for users to provide more detail in a comment box.[166] Samaritans said its Online Safety Lived Experience Panel called for more reporting categories and for an option for 'none of the above'.[167] BILETA said that these reports should be triaged by content moderation for quick review, and Refuge recommended that services should report data on livestream takedowns and moderator responses to us.[168]

Our response

A2.98 We welcome the suggestions of further detail to include in this measure. At this time, we have not included anything further, as we want services to be able to make these types of operational decisions about service design in a way that meets the needs of their service and users. Services must nonetheless ensure that, in doing so, they comply with all our online safety measures to keep users safe on their service.

Further stakeholder responses received on our measure on human content moderation by theme

A2.99 We received additional feedback to our proposed content moderation measure, including:

- Calls for flexibility in the application of the measure;[169]
- Agreement and disagreement with the impact assessment and/or costs;[170]

[165] A member of the Philippine Survivor Network response to the June 2025 Consultation, p.5; Internet Matters response to the June 2025 Consultation, p.6.
[166] A member of the Philippine Survivor Network response to the June 2025 Consultation, p.6; SWGfL response to the June 2025 Consultation, p.9.
[167] Samaritans response to the June 2025 Consultation, p.2.
[168] BILETA response to the June 2025 Consultation, p.5; Refuge response to the June 2025 Consultation, p4.
[169] Meta response to the June 2025 Consultation, p.5; [✂].
[170] A member of the Philippine Survivor Network response to the June 2025 Consultation, p.4; BILETA response to the June 2025 Consultation, p.4; Computer and Communications Industry Association response to the June 2025 Consultation, p.4; Evangelical Alliance UK response to the June 2025 Consultation, p.2; Francis, S response to the June 2025 Consultation, p.4; [✂]; [✂]; Internet Watch Foundation response to the June 2025 Consultation, p.8; Klaushofer, A response to the June 2025 Consultation, p.3; [✂]; Name Withheld 4 response to the June 2025 Consultation, p.2; Name Withheld 11 response to the June 2025 Consultation, p.1; Name Withheld 22 response to the June 2025 Consultation, p.1; Name Withheld 26 response to the June 2025 Consultation, p.3; NPCC response to the June 2025 Consultation, p.2; ODDA response to the June 2025 Consultation, p.2; Open Rights Group response to the June 2025 Consultation, p.8; [✂]; [✂]; Together

- Human Rights/privacy and data concerns;[171]
- Alignment with existing content moderation measures;[172]
- Practicalities associated with the measure;[173]
- Resourcing implications;[174]
- The need for trained moderators;[175]
- The need for human moderators for every livestream;[176]
- Trusted flaggers;[177]
- Moderators intervening in encrypted livestreams;[178]
- Preventing repeat offenders;[179]
- Moderators responding and intervening;[180]
- The need for both human moderation and proactive technology;[181]
- The need for transparency and appeals;[182]
- Human moderation and mental health;[183] and
- Livestreaming containing advertisements.[184]

Our response

A2.100 We thank stakeholders for their input to the proposed measure. We have decided not to proceed with this measure for livestreaming services for the reasons set out in chapter 2: Livestreaming.

Declaration Campaign response to the June 2025 Consultation, p.1; [✂]; [✂] ; UK Finance response to the June 2025 Consultation, p.4; [✂].

[171] [✂]; Name Withheld 19 response to the June 2025 consultation, p.2; Open Rights Group response to the June 2025 Consultation, p.5; [✂].

[172] [✂]; [✂].

[173] Are, C. (Dr) response to the June 2025 Consultation, p.3; Open Rights Group response to the June 2025 Consultation, p.10.

[174] Department for Justice Northern Ireland response to the June 2025 Consultation, p.4; [✂].

[175] CCO response to the June 2025 Consultation, p.5; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.5; IWF response to the June 2025 Consultation, p.7; Samaritans response to the June 2025 Consultation, p.3; Suzy Lamplugh Trust response to the June 2025 Consultation, p.2; [✂]; UK Finance response to the June 2025 Consultation, p.3.

[176] CCO response to the June 2025 Consultation, pp.7-8.

[177] [✂].

[178] IWF response to the June 2025 Consultation, p.5.

[179] SWGfL response to the June 2025 Consultation, p.9.

[180] SWGfL response to the June 2025 Consultation, p.9.

[181] A member of the Philippine Survivor Network response to the June 2025 Consultation, p.4; Barnardo's response to the June 2025 Consultation, p.5; CCO response to the June 2025 Consultation, pp.4-6; Internet Matters response to the June 2025 Consultation, p.3; Lucy Faithfull Foundation response to the June 2025 Consultation, p.2; Online Responsibility Network response to the June 2025 Consultation, p.2; [✂]; [✂].

[182] Francis, S. response to the June 2025 Consultation, p.3; Open Rights Group response to the June 2025 Consultation, p.10.

[183] IWF response to the June 2025 Consultation, p.7; Online Responsibility Network response to the June 2025 Consultation, p.2; Samaritans response to the June 2025 Consultation, p.3; SWGfL response to the June 2025 Consultation, p.8; [✂]; University College London (UCL) Gender and Tech Research Lab response to the June 2025 Consultation, p.4.

[184] We Are Survivors response to the June 2025 Consultation, p.2.

Further stakeholder responses received on our 'Further steps' by theme

Alternative measures

A2.101 In our June 2025 Consultation, we said we would start a programme of stakeholder engagement to ascertain whether there are other options that may further help protect users, including children, from the risks of livestreaming. We also said that we would consider alternative approaches proposed if we considered them to be both proportionate and demonstrably equally or more effective than our current proposals.[185]

A2.102 A number of stakeholders suggested alternative measures to our livestreaming for all users.[186]

A2.103 The IWF said that our approach to the livestreaming measures conflicted with safety by design principles.[187]

A2.104 Open Rights Group suggested we require passive providers to block known offenders from livestream services to prevent re-offence, while ensuring the measure targets only those users.[188]

A2.105 Name Withheld 4 suggested that the use of design frictions, prompts and restrictions would inconvenience legitimate users without stopping harmful uses of livestreaming services.[189]

A2.106 [✂].[190]

A2.107 The NSPCC recommended restricting livestreaming to accounts that had been active for a set period.[191]

A2.108 [✂].[192]

A2.109 The NSPCC welcomed potential proposals for community guideline violations to be used to inform users' ability to broadcast livestreams. It further said that "violations should be considered alongside other data, including a user's age".[193]

A2.110 Name Withheld 9 said that forms of ID verification like confirmation codes to phone or email accounts would be less intrusive than age verification.[194]

A2.111 Several stakeholders provided feedback related to alternative measures that used safety by design approaches.

[185] June 2025 Consultation, chapter 7: Livestreaming – further steps, pp. 70-71.
[186] ACT – The App Association response to the June 2025 Consultation, p.3; C3P response to the June 2025 Consultation, p8; [✂].
[187] IWF response to the June 2025 Consultation, p.5.
[188] Open Rights Group response to the June 2025 Consultation, p.7.
[189] Name Withheld 4 response to the June 2025 Consultation, p.3.
[190] [✂].
[191] NSPCC response to the June 2025 Consultation, p.5.
[192] [✂].
[193] NSPCC response to the June 2025 Consultation, pp.5-6.
[194] Name Withheld 9 response to the June 2025 Consultation, p.3.

A2.112 The UK Interactive Entertainment Association (Ukie) said preventive tools like short broadcast delays and automated keyword detection were already used on major games platforms to allow near-real-time moderation without constant human oversight.[195]

A2.113 Open Rights Group cited an Atlantic Council report saying interoperability lets users choose or design clients that prioritise privacy and security, creating safer experiences. It also welcomed approaches that let users create their own online environments using custom software, such as child-friendly clients.[196]

A2.114 The Antisemitism Policy Trust said there needs to be stronger safety by design measures beyond the crisis response measure.[197]

A2.115 The Suzy Lamplugh Trust said that there were several preventive safety by design measures that can reduce risks to users from livestreaming.[198]

A2.116 [✂].[199]

A2.117 Twitch Interactive Inc. (Twitch) said that user safety risks could be most effectively mitigated through a combination of age-appropriate safeguards, proactive moderation, and user empowerment tools.[200]

A2.118 Image Angel proposed measures to reduce risk without limiting expression or income.[201]

A2.119 5Rights Foundation said technical research showed work was underway on new ways to filter harmful content on livestreams, with potential for real-time content filters.[202]

Going further with the measures

A2.120 In addition to the alternative approaches suggested, some stakeholders suggested that we should explore options for going further with the measures.[203]

A2.121 The OS Network welcomed the proposals to address livestreaming risks but suggested they did not go far enough and described them as a "minimum set of measures" to "set a baseline".[204]

---

[195] Ukie response to the June 2025 Consultation, p.13.
[196] Open Rights Group response to the June 2025 Consultation, p.10.
[197] Antisemitism Policy Trust response to the June 2025 Consultation, p.2.
[198] Suzy Lamplugh Trust response to the June 2025 Consultation, pp.3-4.
[199] [✂].
[200] Twitch response to the June 2025 Consultation, p.8.
[201] Image Angel response to the June 2025 Consultation, p.3.
[202] 5Rights Foundation response to the June 2025 Consultation, p.8.
[203] 5Rights Foundation response to the June 2025 Consultation, p.8; Barnardo's response to the June 2025 Consultation, p.4; CCO response to the June 2025 Consultation, p.8; Check My Ads Institute response to the June 2025 Consultation, pp.3-4; Department of Justice for Northern Ireland response to the June 2025 Consultation, p.5; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.5; Domestic Abuse Commissioner response to the June 2025 Consultation, p.1; [✂]; Evangelical Alliance UK response to the June 2025 Consultation, p.4; [✂]; [✂]; Internet Matters response to the June 2025 Consultation, p.6; Molly Rose Foundation response to the June 2025 Consultation, p.11; Name Withheld 9 response to the June 2025 Consultation, p.3; Name Withheld 26 response to the June 2025 Consultation, p.2; Suzy Lamplugh Trust response to the June 2025 Consultation, pp.3-4; UK Finance response to the June 2025 Consultation, p.3.
[204] OS Network response to the June 2025 Consultation, p.7.

A2.122 The Antisemitism Policy Trust said the provisions should be stronger, with the NSPCC also suggesting it supported all "options for going further".[205]

Our response

A2.123 We thank stakeholders for their alternative proposals. At this stage, we are awaiting the government's decisions on its new legislation regarding restriction of features including livestreaming. We will consider whether any future legislative changes require updates to our current position and will consult before making any such changes as appropriate.

[205] Antisemitism Policy Trust response to the June 2025 Consultation, p.2; NSPCC response to the June 2025 Consultation, p.5.

A3. User sanctions

Further stakeholder responses received on CSEA banning by theme

Increased flexibility for providers

A3.1 Some industry stakeholders called for more discretion for providers or emphasised the importance of providers being able to interpret and enforce their own terms of service.[206] techUK said providers must retain autonomy in interpreting and enforcing their own terms of service to account for the unique community needs, technical capabilities, and operational constraints across services.[207]

Our response

A3.2 While we acknowledge the stakeholder feedback on this issue, we remain of the view that a permanent ban as a default is the most effective way to protect users from child sexual exploitation and abuse (CSEA) harms (see the Effectiveness and benefits section of chapter 3: User sanctions – Measure on banning users for CSEA). The measure already allows for providers to enforce a non-permanent ban in limited exceptional circumstances. Regarding comments on terms of service, we consider that our measure allows providers to interpret and enforce their terms of service. For example, providers have discretion as to the technical implementation of a ban and the method for preventing users from returning to the service. We have also included CSEA content proxy in the measure to ensure that providers can benefit from the 'safe harbour' of complying with the Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes), even when they have applied their terms of service (rather than making an illegal content judgement).

Requests for wider/alternative safeguarding actions

A3.3 Civil society stakeholders including the Internet Watch Foundation (IWF) and Internet Matters asked us to consider the use of deterrence messaging following a ban as a means of educating adult perpetrators and signposting to support, identifying the Lucy Faithfull Foundation's 'Stop It Now' service as an example of best practice.[208]

A3.4 Stakeholders also highlighted the need to report to law enforcement and/or other statutory services alongside user banning.[209] The National Police Chiefs' Council (NPCC)

---

[206] [✂]; Google LLC. response to the June 2025 Additional Safety Measures Consultation (June 2025 Consultation), p.30; [✂]; [✂].

[207] techUK response to the June 2025 Additional Safety Measures Consultation, p.23.

[208] Internet Matters response to the June 2025 Additional Safety Measures Consultation, p.13; Internet Watch Foundation (IWF) response to the June 2025 Additional Safety Measures Consultation, p.45; Lucy Faithfull Foundation response to the June 2025 Additional Safety Measures Consultation, pp.8-9; [✂]; Online Safety Network response to the June 2025 Additional Safety Measures Consultation, p.22; Refuge response to the June 2025 Additional Safety Measures Consultation, p.14; Scottish Government response to the June 2025 Additional Safety Measures Consultation, p.3.

[209] Office of the Children's Commissioner for England response to the June 2025 Additional Safety Measures Consultation, p.20; Scottish Government response to the June 2025 Additional Safety Measures Consultation, p.3; [✂]; [✂].

stated the need for the measure to be approached with a parallel process for referral to law enforcement when offending is identified.[210]

A3.5 Service providers said there was a need for wider measures including service level sanctions and upload prevention alongside the application of a ban to prevent the circulation of child sexual abuse material (CSAM).[211]

Our response

A3.6 Under section 66 of the Online Safety Act 2023 (the Act), service providers are required to report any UK-linked CSEA to the National Crime Agency (NCA). This measure does not impact on this requirement, and providers remain responsible for reporting CSEA in addition to banning users who have posted CSEA on the service or knowingly received it.

A3.7 We recognise the value in promoting channels for rehabilitation and support. However, we also acknowledge the potential risks with this approach. We are concerned that:

- Deterrence messaging may alert users to the reason for their ban which may impact on any criminal investigation.
- Evidence into the effectiveness of warning messages to create behaviour change amongst CSEA offenders shows mixed results. In the Protect Children, Tell Me About Tech research, encounters with online messages was seen to provoke a variety of responses ranging from indifference to behaviour change.[212] Similarly while many studies show that behaviour can be modified through the use of a warning, research highlights the importance of the design of deterrence messaging to maximise effectiveness with messages needing to be clearly communicated and well-timed.[213] Currently, the lack of evidence as to the factors that increase receptiveness and the limited application of such warnings restrict our ability to assess effectiveness and make appropriate recommendations on implementation.
- The cost implications to recommend this across all user-to-user services (as per the current application of the measure) could be significant.

A3.8 As such, we are not currently recommending anything further in this space. However, service providers may choose to use this kind of messaging where they have the capabilities to adopt it for adult perpetrators or for children, as discussed in the section 'Alternative sanctions and wider safeguarding actions.'

Request for cross-platform information sharing

A3.9 Civil society stakeholders welcomed the decision to extend a ban to all regulated user-to-user services operated by a provider and encouraged us to go further in encouraging wider information sharing across services.[214]

---

[210] National Police Chiefs' Council (NPCC) response to the June 2025 Additional Safety Measures Consultation, p.11.
[211] IWF response to the June 2025 Consultation, p.45; Scottish Government response to the June 2025 Consultation, p.3.
[212] Protect Children, 2026. CSAM perpetrator Research Project: Findings from a Survey of CSAM Perpetrators on Digital Platform Use and Design (Tell Me More About Tech).
[213] Protect Children, 2025. Online Warning Messages for CSAM prevention: Evidence and Practice Mapping.
[214] Commissioner Designate for Victims of Crime Northern Ireland response to the June 2025 Additional Safety Measures Consultation, p.7; IWF response to the June 2025 Consultation, p.44; Lucy Faithfull Foundation response to the June 2025 Consultation, p.8; Marie Collins Foundation response to the June 2025 Additional Safety Measures Consultation, p.9; National Society for the Prevention of Cruelty to Children (NSPCC) response

Our response

A3.10 We recognise the concerns raised in the June 2025 Additional Safety Measures Consultation (June 2025 Consultation) relating to banned users migrating to other services to continue offending. We consider that our recommendation that this measure applies to all user-to-user services goes some way to mitigate this risk and acknowledge how cross-service information sharing could potentially help to go further. However, we are also aware of technical barriers and data protection challenges that hinder some services' ability to share information safely. As such, we are not currently able to recommend this as part of this measure as this would need additional assessment and consultation. Nonetheless, we would encourage any services with the ability to do so to consider information sharing through programmes such as Lantern.[215]

Proposals to expand the scope of this measure

A3.11 Civil society stakeholders outlined the value of extending the user banning measure to cover other types of illegal content, particularly non-consensual intimate image abuse.[216]

Our response

A3.12 We have focussed this measure on CSEA due to the severity of the harm, the high rate of recidivism and the evidence demonstrating the pervasive nature of perpetrating. We also note the degree of international alignment on the importance of combatting this harm. Despite this, we recognise the significant harm caused by other forms of illegal content and recommend a general policy concerning sanctions for these as outlined in chapter 3: User sanctions. In addition, in May, we published our statement on Detecting intimate image abuse, which recommends the use of proactive technology to detect such content.[217]

Engaging with children

A3.13 5Rights Foundation suggested we engaged with children and ensured their feedback is captured as part of our evidence gathering.[218]

Our response

A3.14 We have conducted a workshop with children to obtain their views on this measure (see paragraph 3.75 of chapter 3: User sanctions – Measure on banning users for CSEA). We have taken their views along with further evidence supplied by civil society through the consultation into account when finalising our decisions, in particular our decision to pursue a more nuanced approach to children.

Further recommendations

A3.15 Internet Matters made several further recommendations relating to the measure, including around moderators, appeals, and supporting parents.[219]

---

to the June 2025 Additional Safety Measures Consultation, pp.39-40; Online Safety Network response to the June 2025 Consultation, p.23; Refuge response to the June 2025 Consultation, p.14.

[215] Tech Coalition, 2023. Announcing Lantern: The First Child Safety Cross-Platform Signal Sharing Program.

[216] British and Irish Law Education Technology Association (BILETA) response to the June 2025 Additional Safety Measures Consultation, p.24; [✂]; Online Safety Network response to the June 2025 Consultation, p.22; Refuge response to the June 2025 Consultation, pp.14-15.

[217] Ofcom (2026), May 2026 Statement, Detecting Intimate Image Abuse.

[218] 5Rights Foundation response to the June 2025 Additional Safety Measures Consultation, p.12.

[219] Internet Matters response to the June 2025 Consultation, pp.14-15.

A3.16 Government and law enforcement stakeholders provided some suggestions around technical tools that could be used to improve the effectiveness of a ban.[220] The NPCC said providers should make best use of technology which works proactively to ensure that a ban tracks the user through all available means (such as IP address), as well as safety measures ensuring children are not permitted to share SGII with others in the first place.[221] A government stakeholder said there should be a strong ask for preventative mechanisms to stop re-registration, such as device fingerprinting or behavioural detection.[222]

Our response

A3.17 We will consider whether any future legislative changes require updates to our current position and will consult before making any such changes as appropriate.

A3.18 With regard to the technical tools which could be used, we have explained our reasoning in chapter 3: User sanctions – Measure on banning users for CSEA for recommending providers have discretion over the technical steps they take to implement the measure and recognise there are a range of tools which may be used to prevent a user from returning.

Further stakeholder responses received on our user sanctions measures by theme

Education and reform

A3.19 Six civil society stakeholders asked for us to highlight the importance of educational prompts and supportive interventions when setting out possible sanctions.[223] These stakeholders highlighted the importance of allowing users to amend their behaviour, particularly child users.

A3.20 Open Rights Group raised concerns about lifetime bans, noting that criminal law allows for character reform and it is unclear how banned users could regain access or how providers would coordinate with probation services and law enforcement. It warned that this could give considerable power to service providers to impact user interaction with things like government services.[224]

A3.21 In contrast, Refuge said that sanctions like educational prompts and strikes may not be appropriate in some cases for VAWG-related offences. It said such sanctions may be too weak to stop determined perpetrators, and asked Ofcom to ensure sanctions for offences related to VAWG are strong enough to prevent ongoing harm.[225]

---

[220] C3P response to the June 2025 Additional Safety Measures Consultation, pp.15-16; Department of Justice for Northern Ireland response to the June 2025 Additional Safety Measures Consultation, p.13; [✂]; Information Commission's Office (ICO) response to the June 2025 Consultation, pp.23-24; NPCC response to the June 2025 Consultation, p.10.

[221] NPCC response to the June 2025 Consultation, p.11; NPCC response (Letter) to the June 2025 Consultation, p.2.

[222] [✂].

[223] Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.13; Evangelical Alliance response to the June 2025 Consultation, p.9; Internet Matters response to the June 2025 Consultation, pp.15-16; IWF response to the June 2025 Consultation, p.49; Open Rights Group response to the June 2025 Consultation, pp.34-35; Samaritans response to the June 2025 Consultation, p.9.

[224] Open Rights Group response to the June 2025 Consultation, pp.34-35.

[225] Refuge response to the June 2025 Consultation, pp.16-17.

Our response

A3.22 For the most part, our measures are not prescriptive about the sanctions a provider should apply. Where we have specified sanctions such as the measure on banning users for CSEA, this is due to our assessment of appropriate mitigations to those harms.

A3.23 Our measures allow providers to prioritise education and reform, while giving them flexibility to escalate sanctions, and implement firmer first sanctions when deemed appropriate.

A3.24 The following themes are explained in our June 2025 Consultation and are discussed in chapter 3: User sanctions – Measures on user sanctions policy at several points:

c) Information and educational prompts are included in our non-exhaustive list of sanctions providers may use (see table 3.1).

d) We set out several relevant points in outlining the factors in our measures:

i) Providers may consider whether the user was provided with sufficient information as to why they were sanctioned and whether the user had the opportunity to appeal. [See "Whether the user has previously generated, uploaded, or shared relevant content, including whether they were sanctioned for doing so".]

ii) Providers may consider the nature of the relevant harm when judging the potential impact of the sanction on the user and take a nuanced approach. For example, this may include considering the potential vulnerability of the user, as well as whether they are a child. [see section "Potential impact of the type and duration of the sanction on the user being sanctioned".]

iii) Providers may give information and educational prompts to users alongside another sanction. [see Table 3.1].

e) Furthermore, our measures recommend that providers include information about their sanctions policy in their terms of service to be transparent with users. See chapter 3: Amendments to the Codes to reflect user sanctions measures for further information.

A3.25 Taken together, these points demonstrate how the measures allow for the use of educational interventions and affirms their importance.

A3.26 In response to Open Rights Group's concerns, the scope of these measures is the setting of a sanctions policy and not a criminal judgment. It is up to an individual provider to determine whether to impose a ban and if so its duration, and how they wish to use sanctions and other actions together, including opportunities for reform (as set out in the chapter). As set out above, where we do set out specific sanctions in other measures, we have done so following an assessment of the harm and possible mitigations.

A3.27 We are not recommending that providers apply lifetime bans but are noting that, where they choose to do so, we would expect them to have considered the factors we set out in chapter 3: User sanctions – Measures on user sanctions policy to ensure such a ban would be appropriate. The inclusion of recommended factors in our measures will also assist providers in producing proportionate sanctions policies; in balancing the considerations of the severity of the harm, the impact on the user, and any previous violations, providers should be guided to apply sanctions appropriately. This includes where sanctions may impact access to certain services.

A3.28 We set out our analysis of the impact on users' freedom of expression and freedom of association in the section 'Rights impact' in chapter 3: User sanctions – Measures on user sanctions policy.

A3.29 In response to Refuge's concerns, in our November 2025 Statement: A Safer Life Online for Women and Girls (November 2025 Statement) we outline good practice that providers should consider when mitigating violence against women and girls, including taking steps to identify and prevent the creation of new accounts by perpetrators who may do so to evade a sanction or a ban. This guidance is complementary to our measures in aiding providers in the development and implementation of their sanctions policies.

A3.30 We therefore consider that these measures allow providers to use appropriate sanctions and make decisions about their policies that are most suited for their services. We also consider that these measures allow and guide providers in setting appropriate sanctions, without recommending unnecessarily severe restrictions. As such, we have not made any changes to our proposed measures because of these responses.

Requests for flexibility and prescriptiveness in design of measures

A3.31 In response to the June 2025 Consultation, we received a range of feedback from stakeholders in regard to implementing the measures.

A3.32 Four industry stakeholders and the Evangelical Alliance welcomed and noted the importance of providing flexibility for providers when implementing sanctions policies.[226]

A3.33 Four stakeholders said sanctions should be tailored to the individual service and that Ofcom should allow for this flexibility.[227]

A3.34 In contrast, several stakeholders highlighted the importance of consistency in how sanctions are applied across services. They warned that inconsistent application may negatively impact users and reduce the benefits of the measure.[228] Barnardo's suggested that Ofcom produce guidance to ensure consistency in how sanctions are applied across services.

A3.35 Two stakeholders warned of unintended impacts on users from lack of balance between flexibility and prescriptions could deter online participation.[229]

Our response

Flexibility

A3.36 Our measures already offer providers the flexibility to apply their policy in a way that best fits their services, while achieving consistent application.

A3.37 Key to this overall flexibility is providing a non-exhaustive, illustrative list of the range of sanctions possible, not specifically recommending any of these in our measures and setting out factors that give providers a recommended framework for their policy. We expect that the range of sanctions a provider may impose will likely depend on that service's functionalities, and so the measures would already address concerns from stakeholders regarding the measures being too prescriptive for some types of services.

---

[226] Evangelical Alliance response to the June 2025 Consultation, p.9; GitHub response to the June 2025 Consultation, pp.7-8; Meta response to the June 2025 Consultation, p.12; [✂]; [✂].
[227] [✂]; [✂]; [✂]; We Are Survivors response to the June 2025 Consultation, p.7.
[228] Barnardo's response to the June 2025 Consultation, p.16; BILETA response to the June 2025 Consultation, pp.28-29.
[229] Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.14; GitHub response to the June 2025 Consultation, pp.7-8.

A3.38 We also acknowledge that, in some cases, service providers may choose to just action content and not apply a sanction. This does not constrain providers into enforcing user level sanctions in cases where they deem it inappropriate, addressing stakeholders' requests for balance and nuance.

A3.39 The Act also provides flexibility for those who do not wish to adopt the measures, allowing them to adopt alternative measures to meet their duties.[230]

Consistency

A3.40 On the subject of stakeholders requesting consistency across services, we have already set out points which provide individual services with a framework that will result in this:

a) We have set a clear objective that all in-scope services will need to achieve – preventing future dissemination of illegal content/content harmful to children.
b) We have set out three factors that all in-scope providers should consider. We expect this to create some alignment between the approach on different services.
c) We have already said that the policy should be reviewed to remain fit for purpose for the service. We would expect that providers revisiting and adjusting their sanctions policy would mean that these policies can be adapted to be consistent even where risk and harms are changing.

A3.41 We recognise that there is a trade-off in giving providers, and that this may allow providers to apply different sanctions in similar cases on different services. However, because of the variation in factors like service type, capacity and user base, flexibility should mean providers create a more appropriate and effective policy. Given the evidence outlined in the section titled 'Effectiveness and benefits' in chapter 3: User sanctions – Measure on user sanctions policy, and the diversity of services, being more prescriptive may limit the effectiveness and proportionality of the measures as it may mean service providers adopt a policy that is not suited for the design of their service, or its risk profile.

A3.42 We also expect stakeholders' concern about inconsistent determination around content harmful to children would be addressed by guidance we produced for providers on identifying this content, and that broadly the Act sets out expectations regarding mitigating relevant harms.[231]

Unintended outcomes

A3.43 Regarding stakeholder responses around unintended outcomes, our measures are sufficiently flexible to allow providers to design their policy in such a way that strikes the right balance between enforcing sanctions and user's rights. We address the impact on users' rights in our 'Rights impact' section in chapter 3: User sanctions – Measure on user sanctions policy. We consider that concerns regarding unintended consequences which would impact online participation are addressed by the measures' provisions for flexibility and consistency.

A3.44 We will therefore proceed with the measures as set out in our June 2025 Consultation, providing both flexibility and clear guidance for providers.

---

[230] Where providers take alternative measures, they must keep a record of what they have done and explain how the relevant safety duties have been met. The Act provides that, in doing so, they must consider the importance of protecting users' rights to freedom of expression within the law and of protecting users from breaches of relevant privacy laws. We set out what providers should record when taking alternative measures in our Record-Keeping and Review Guidance.
[231] Guidance on Content Harmful to Children; Section 12 of the Act.

Intent as an additional factor

A3.45 Three civil society groups, one individual, and another stakeholder suggested the proposed measures should recommend consideration of a user's intent.[232] Snap, Inc. said it considered intent when deciding enforcement actions.[233]

A3.46 The National Society for the Prevention of Cruelty to Children (NSPCC) and Samaritans highlighted suicide, self-harm and eating disorder content harmful to children in particular as needing careful consideration of intent, due to the nature of the harm.[234]

Our response

A3.47 We understand that by 'intent', stakeholders were referring to the culpability of the individual who posted the relevant content. We agree that a user who deliberately posts content in order to cause harm is more culpable than a user who unknowingly posts harmful content, and that a higher degree of culpability may warrant a harsher sanction. For example, a user who posts a step-by-step eating disorder instruction manual is more culpable and therefore may deserve a more severe sanction than a user who posts recovery eating disorder content which unintentionally provides instructions. We understand stakeholders to have been commenting on both the illegal content and protection of children sanctions measures when referring to intent.

A3.48 We consider the proposed measures already permit service providers to take intent and culpability into account when considering the impact of the type and duration of sanction on the posting. A provider may take the view that the potential impact of a particular sanction on a user who did not intend to cause harm would be greater and less justified than on a user who did intend to cause harm, and therefore impose lighter sanctions on users who unintentionally or unknowingly post harmful content. Service providers may also take intent into account when considering appeals against sanctions, adjusting the sanction accordingly. By considering the impact of the type and duration of a sanction on the posting user, providers will be able to give careful consideration to the treatment of users who generate, upload, or share suicide and self-harm content, as raised by Barnardo's, the NSPCC, and Samaritans.

A3.49 Furthermore, as set out in our June 2025 Consultation and in chapter 3: User sanctions – Measure on user sanctions policy, the Protection of Children Code recommends that providers in scope of measure PCU F4 should signpost children to resources when they post suicide, self-harm, eating disorder or bullying content harmful to children. Our Children's Register of Risks and Guidance on Content Harmful to Children set out our approach to handling the difficult nuances which come with determining content harmful to children which is suicide, self-harm and eating disorder content.

A3.50 In addition, we consider that including intent or culpability as a standalone factor for providers to consider could materially increase the burden on them, as it will not always be relevant to a particular harm or scenario. While providers may take a view on the user's intent when considering whether they have previously posted relevant content, for example repeat instances may suggest that the user did intend to cause harm, they will not

[232] Barnardo's response to the June 2025 Consultation, pp.15-16; Cook, J. response to the June 2025 Consultation, p.2; [✂]; Samaritans response to the June 2025 Consultation, p.9; Which? response to the June 2025 Consultation, pp.14-15.
[233] Snap Inc. response to the June 2025 Consultation, p.15.
[234] NSPCC response to the June 2025 Consultation, p.46; Samaritans response to the June 2025 Consultation, p.9.

always have evidence of the user's culpability. Where intent is relevant, we are satisfied that, for the reasons set out in the previous paragraphs, the measures as proposed permit providers to take it into account when setting and applying their policy. We will therefore not be including intent or culpability as a standalone factor for providers to consider.

Further specific harms requests

A3.51 Three stakeholders asked for the measures to include harms specific requirements for offences related to violence against women and girls (VAWG).[235]

Our response

A3.52 Providers may choose to implement more severe sanctions for specific harms – this includes VAWG-related offences. We consider that our measures already account for this.

A3.53 We will consider whether any future legislative changes require updates to our current position and will consult before making any such changes as appropriate.

Additions to the measure – information-sharing as part of sanctions policy

A3.54 Three stakeholders suggested the measures include the recommendation that providers share information on sanctioned users across services.[236]

Our response

A3.55 We acknowledge evidence of industry practice in this area and providers considering it across their services. Providers are free to sanction across multiple services, and may also share information of their own volition, however this does not form part of this measure.

Additions to the measure – reporting to authorities

A3.56 Two stakeholders said the measures should set out that providers should report users who repeatedly contravene terms of service to law enforcement authorities.[237]

Our response

A3.57 Reporting to law enforcement is out of scope of the Act, excluding duties around CSEA,[238] but providers may choose to do this where they consider it appropriate.

Additions to the measure – user verification

A3.58 One stakeholder suggested the use of identity verification, to verify the autonomy of sex workers before application of severe sanctions, and to prevent sanctioned users returning to service, which it says is a key enabler for large-scale fraud.[239]

Our response

A3.59 Providers may choose to use identity verification information (IDV) as a means for determining appropriate sanctions, but specifying the use of IDV would be inconsistent

---

[235] [✂]; Refuge response to the June 2025 Consultation, p.16; Suzy Lamplugh Trust response to the June 2025 Consultation, p.7.
[236] ASA response to the June 2025 Consultation, pp.11-12; Suzy Lamplugh Trust response to the June 2025 Consultation, p.7; UK finance response to the June 2025 Consultation, p.13.
[237] [✂]; UK Finance response to the June 2025 Consultation, p.13.
[238] Section 66 of the Act.
[239] NCA response to the June 2025 Consultation, p.19.

with our approach of being flexible in the application of the measure. Regardless, we do not believe at this stage there to be a case for including IDV in the sanctions measure. Our Additional Duties Consultation for categorised services has set out our proposals around identity verification in relation to duties on Category 1 services to offer optional identity verification.[240]

A3.60 We will consider these points when assessing the proportionality of any options for future measures.

Additions to measure – impact

A3.61 In response to our factor on impact on users, four civil society stakeholders stressed the importance of providers considering the impact of sanctions on children when setting their sanctions policy.[241]

Our response

A3.62 We expect our measures already allow for this. In setting out the factor around impact on users, in chapter 3: User sanctions, we have said that one of the things providers may consider is whether they have reasonable grounds to believe the user is a child, and the impact the sanction may have on that user in light of their age.

Applying the user sanctions policy

A3.63 One industry stakeholder sought clarity on whether the measure proposed that the policy on user sanctions was internal only, or needed to be published by the service.[242]

Our response

A3.64 As set out in the section titled 'How these measures work' of chapter 3: User sanctions – Measure on user sanctions policy, we did not propose that the full detailed policy should be included in external publications, such as terms of service, and have confirmed this proposal. However, providers should include information on their sanctions policy in their terms of service.

Need for independent adjudicators and oversight

A3.65 Three stakeholders asked for the measures to include, or provide clarity on, an independent oversight mechanism to protect user rights.[243] Open Rights Group said that they consider the measures potentially infringe the Article 6 European Commission of Human Rights (ECHR) right to a fair trial.

Our response

A3.66 We have considered the impact of the measure on users' rights in detail in our rights assessment in chapter 3: User sanctions – Measure on user sanctions policy. We consider that there are sufficient safeguards in place to protect users' rights, and to provide appropriate avenues of appeal to users impacted by the policy sanctions measures. We do

[240] Sections 64 and 65 of the Act.
[241] Barnardo's response to the June 2025 Consultation, pp.15-16; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, pp.13-14; NSPCC response to the June 2025 Consultation, p.46.
[242] Hammy Media Ltd. response to the June 2025 Consultation, p.12.
[243] Cook, J. response to the June 2025 Consultation, p.1; [✂]; Open Rights Group response to the June 2025 Consultation, pp.35-36.

not consider this call for independent adjudicators raises any additional points relevant to the design of the measure which are not already accounted for by the safeguards in place, and considered in our rights assessment. We are therefore satisfied that the measures are proportionate and have decided not to make any amendments in light of these stakeholder responses.

Limitations of the sanctions

A3.67 Several stakeholders raised that the sanction of permanent bans may be limited in effectiveness where users can easily return to the service.[244] Others raised the issue of users easily regaining access to services via new or separate accounts or using means like virtual private networks (VPNs) to bypass sanctions.[245]

A3.68 The British and Irish Law Education and Technology Association (BILETA) raised that where accounts are sanctioned or banned, users may be able to create new accounts to circumvent the ban and said that additional recommendations regarding limiting a user's ability to create accounts would increase the impact of the proposed measure.[246]

A3.69 Refuge stated that effective user sanctions depend on good reporting and appeals systems, explaining that survivors often find reporting exhausting, especially when abuse comes from multiple accounts.[247]

Our response

A3.70 Regarding returning to service, we addressed this issue in our June 2025 Consultation in the context of Measure ICU H3 (banning users for CSEA).[248] We said it would support the effectiveness of a ban to prevent users from returning; the same applies in the user sanctions policy context; where providers want to ban users permanently, we would expect providers to take reasonable steps in their policies to achieve this.

A3.71 However, we also noted there that there is unlikely to be an appropriate 'one size fits all' approach for preventing return across in-scope services, that technology in this space is ever changing, and there is a high risk that recommending methods as part of the measures in our Illegal Content and Protection of Children Codes could aid those looking to circumvent sanctions.

A3.72 We therefore conclude that, where services do implement bans with the intention of removing users' access to services permanently in relation to these measures, there is a benefit for providers in ensuring methods are in place to effectively enforce these bans, such as methods of preventing return to service.

---

[244] BILETA response to the June 2025 Consultation, pp.28-29; FCA response to the June 2025 Consultation, p.6; [✂]; [✂]; Refuge response to the June 2025 Consultation, pp.15-16; UK finance response to the June 2025 Consultation, p.13.

[245] BILETA response to the June 2025 Consultation, p.28; FCA response to the June 2025 Consultation, p.6, [✂]; Refuge response to the June 2025 Consultation, pp.16-17; We Are Survivors response to the June 2025 Consultation, p.7.

[246] BILETA response to the June 2025 Consultation, p.23.

[247] Refuge response to the June 2025 Consultation, pp.16-17.

[248] June 2025 Consultation, chapter 15: User banning and preventing return following detection of child sexual exploitation and abuse content, p.194

A3.73 We also agree with the point raised by Which? and [✂] that banning can provide an effective momentary disruption, even if some users are able to circumvent the ban and return to the service.[249]

A3.74 On Refuge's point, these measures make up a range of measures across our Illegal Content and Protection of Children Codes, including several reporting and complaints measures that are intended to support users in easily reporting content and other users. As set out in the explanation of the measure in chapter 3: User sanctions – Measure on user sanctions policy, we expect providers to consider their sanctions policy when they have identified relevant content through means such as reports.

Reporting duty

A3.75 The NPCC recommended that we introduce a compliance reporting duty, requiring services to publish metrics on ban evasion, reoffending, and enforcement outcomes.[250]

Our response

A3.76 We would need to assess any options for new measures carefully before recommending them in our Illegal Content or Protection of Children Codes. We will not be pursuing this at this time, however we acknowledge transparency duties may lead to categorised service providers including such information in their transparency reports.

Multiple accounts

A3.77 BILETA raised concerns about repeat contraventions and welcomed proposals clarifying how users with multiple accounts would be handled under these rules.[251] Another stakeholder suggested technology for removing linked accounts.[252]

Our response

A3.78 We have said that a history of sharing harmful content is a factor providers should consider when setting their sanctions policy, and that the policy applies to 'users' rather than just 'accounts'. However, it is up to providers to decide which sanctions would most effectively mitigate the risks of harmful content on their service. This may include taking action against all of a user's accounts on the service.

Hacked accounts

A3.79 The Advertising Standards Authority (ASA) noted that in cases of hacked accounts used for scams, sanctions may provide a disruption but result in the original owner of the account being sanctioned when the fraudster moves on.[253] An individual respondent also raised that the measures did not consider hacked accounts.[254]

Our response

A3.80 We did not discuss hacked accounts in our June 2025 Consultation. The flexibility of the factors sets out in our measures allow providers to consider how harms manifest on their service, including those that would lead to hacked accounts. They therefore could take this

[249] [✂]; Which? response to the June 2025 Consultation, p.15.
[250] NPCC response to the June 2025 Consultation, pp.10-12.
[251] BILETA response to the June 2025 Consultation, p.29.
[252] [✂].
[253] ASA response to the June 2025 Consultation, p.12.
[254] Name Withheld 9 response to the June 2025 Consultation, p.9.

into account when setting their individual policy. There is also benefit to our recommended appeals mechanism as users whose accounts are hacked and sanctioned could appeal.

Bot accounts

A3.81 BILETA asked for information on how bot accounts would be recognised and sanctions applied.[255]

Our response

A3.82 It is up to providers to decide which sanctions would most effectively mitigate the risks of harmful content on their service This includes where providers identify bots as a potential source of harmful content. The Act also sets out that bots or other automated tools are to be regarded as users if their functions include interacting with user-generated content and they are not controlled by or on behalf of the service provider.[256] In those circumstances, bots would be in scope of the measure. For further guidance on bots, and evidence of their risks, please see our Illegal Content Judgements Guidance, Illegal Harms Register of Risks, and Children's Register of Risks.

Individuals versus commercial entities

A3.83 The ASA stated that the proposals "do not distinguish between those posting as individuals and those posting with commercial intent".[257]

Our response

A3.84 For the avoidance of doubt, the measures apply to UK users, which can be either an individual in the UK or an entity formed under the laws of the UK.[258]

Content moderation

A3.85 The Association of British Insurers (ABI) recommended Ofcom require services to remove illegal content, rather than leaving it to service discretion. BILETA noted that focusing sanctions on users who create and share harmful content diverges from the Act's broader emphasis on provider responsibility.[259]

A3.86 One stakeholder considered sanctions should not be applied to proxy content only explicitly illegal content.[260]

A3.87 The NCA questioned whether Ofcom can effectively check and challenge provider's claims concerning their resources.[261]

Our response

A3.88 The Act already requires services to remove illegal content of which they are aware. Our content moderation measures ICU C1 and C2 set out our recommendations for providers in following this duty.

A3.89 In response to BILETA, as stated in our June 2025 Consultation, the measure is a means for services to meet their duties under the Act in relation to sections 10(2) and 12(2) and (3) of

[255] BILETA response to the June 2025 Consultation, p.23.
[256] Section 55(4)(b) of the Act.
[257] ASA response to the June 2025 Consultation, p.11.
[258] Section 227(1) of the Act.
[259] ABI response to the June 2025 Consultation, p.3; BILETA response to the June 2025 Consultation, p28.
[260] [✂].
[261] NCA response to the June 2025 Consultation, p.20.

the Act, in relation to policies on user access to the service (see sections 10(4)(d) and 12(8)(d)). Further, the intent of the measure is to reduce illegal content on service, and content harmful to children where the provider chooses to prohibit that content.

A3.90 Recommending the sanctions policy covers content proxy is consistent with our content moderation measures. As we set out in our December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement) and in our April 2025 Statement on Protecting Children from Harms Online (April 2025 Statement),[262] we know providers may moderate content by reference to their terms of service where they are satisfied that they cover illegal content and content harmful to children, rather than make judgements on that content. Our content moderation measures cover content proxy to ensure that providers that take this approach are in scope of the Illegal Content and Protection of Children Codes. Recommending that the sanctions policy apply only where a provider makes a content judgement would limit the effectiveness of the measures by excluding all instances where providers moderate content by applying their terms of service.

A3.91 Regarding resourcing, our existing content moderation measures recommend providers ensure their resourcing gives effect to their internal policies and performance targets. We think this sets a standard in this area.[263] We will take appropriate enforcement action if we do not consider that our measures or suitable alternatives are being followed. In doing this, we will follow our processes and procedures, which include using our information gathering powers where appropriate, and considering representations made by the provider.

Quantification of cost estimates

A3.92 One stakeholder considered that a precise cost quantification is not feasible at this stage.[264]

Our response

A3.93 In our June 2025 Consultation, we said that we expected costs to vary widely across service providers depending on factors such as service size, level of risk, type of sanction, how the service provider chooses to implement it, and existing systems and processes in place. While we are not able to calculate a precise cost estimate for all types of service providers, we are satisfied that the potential costs for the services in scope of this measure are proportionate.

Human moderator training costs

A3.94 BILETA noted that increased training costs for content moderators could lead to greater reliance on automation.[265]

[262] Ofcom (2024), December 2024 Statement, Protecting People from Illegal Harms Online, Vol.2, chapter 2: Content Moderation; Ofcom (2025), April 2025 Statement, Vol.4, chapter 14: Content moderation for user-to-user services.
[263] Illegal Content Codes of Practice (Illegal Content Codes), Measures ICU C4 and ICU C6; Protection of Children Codes of Practice (Protection of Children Codes), Measures PCU C4 and PCU C6.
[264] Snap, Inc. response to the June 2025 Consultation, pp.15.
[265] BILETA response to the June 2025 Consultation, p. 30.

Our response

A3.95 We acknowledge that these measures could increase the costs of providing training to individuals working in content moderation, but it is not clear that this would necessarily lead to a greater reliance on automation.

A3.96 We note that an increased reliance on automation in content moderation could be beneficial as it may be more cost-effective for some services and will not necessarily result in a reduction in content moderation performance.

Package of measures

A3.97 The Children's Commissioner's Office (CCO) said that the measure alone would not prevent systematic harms and should therefore be recommended as part of a package of measures.[266]

Our response

A3.98 The measures are part of the wider Illegal Content Codes and the Protection of Children Code. They have direct interaction with other measures, such as our reporting and complaints measures, terms of service measures, and content moderation measures. Furthermore, we consider that the decisions in this statement will ensure a significantly safer environment online for all users, in particular children. We will be closely monitoring how service providers implement the measures in the Codes. This will enable us to identify any gaps in protections for children, to inform our prioritisation of future work to strengthen our Codes.

Definitions

A3.99 UK Finance raised that the proposed measures do not define what a severe harm is, in the context of fraud. A government stakeholder recommended that Ofcom provide clear definitions for 'sanction' and 'suspected illegal content'.[267]

Our response

A3.100 We discussed severity of harm in of chapter 3: User Sanctions, where we provided multiple possible interpretations for providers. This allows for diversity of services and the differing ways risk and harm can manifest.

A3.101 The term 'sanction' is defined in the definition and interpretation section of the Codes glossaries. We do not use the term 'suspected illegal content' in the measure or the chapter.

General disagreement with measures

A3.102 Two stakeholders disagreed with the measure, providing no evidence or defined reason.[268]

Our response

A3.103 As these responses did not include any evidence to support their disagreement, or provide feedback on specific measures, we have not made any changes to our proposals as a result.

---

[266] CCO response to the June 2025 Consultation, p.20.
[267] [✂]; UK Finance response to our June 2025 Consultation, p. 13.
[268] Luethje, Y. response to the June 2025 Consultation, p.7; [✂].

Further stakeholder responses received on amendments to the Codes to reflect user sanctions measures by theme

Feedback on the appeals amendments

A3.104 The Information Commission's office (ICO) supported the proposed amendments but requested confirmation regarding the incorporation into the measures of our proposal to recommend that providers consider the appropriateness of the sanction that has been applied when determining appeals.[269]

A3.105 Multiple stakeholders also highlighted the importance of appeals as part of a sanctions process:

d) UK Finance noted that, due to the financial or reputational stakes of fraud, related sanctions are more likely to be contested.[270]
e) Snap, Inc. said it has mechanisms in place to ensure users understand any actions taken against them or their account, and the opportunity to dispute enforcement outcomes.[271]

A3.106 Two individuals urged the importance of user redress in ensuring accountability and, asked for clarity regarding how the measures ensure these points for individuals and small organisations.[272]

Our response

A3.107 This feedback highlights the importance of these changes.

A3.108 We welcome the ICO's feedback, and confirm this amendment is incorporated at measure ICU D10A.

Feedback on terms of service amendments

A3.109 In response to our June 2025 Consultation, the ICO agreed with the proposed amendments, and Internet matters agreed with the importance of providers being transparent with users regarding sanctions.[273] [✂] called for independent oversight, transparency, and user redress mechanisms to ensure accountability.[274] Snap, Inc. shared its considerations when balancing transparency and providing information that may enable circumvention of sanctions.[275]

Our response

A3.110 As we said in previous statements, we agree that publishing detailed internal content policies could aid offenders.[276] We acknowledge the need for providers to find a balance between transparency and not aiding offenders. In our view, a measure that recommends

[269] ICO response to the June 2025 Consultation, p.26.
[270] UK Finance response to the June 2025 Consultation, p.14.
[271] Snap, Inc. response to the June 2025 Consultation, p.15.
[272] Cook, J. response to the June 2025 Consultation, p.2; [✂].
[273] ICO response to the June 2025 Consultation, p.25; Internet Matters response to the June 2025 Consultation, p.15.
[274] [✂].
[275] Snap, Inc. response to the June 2025 Consultation, pp.14-15.
[276] Ofcom (2024), December 2024 Statement, Vol.2, chapter 2: Content moderation; Ofcom (2025), April 2025 Statement, Vol.4, chapter 14: Content moderation for user to-user services.

providers include information about their sanctions policy in their terms of service strikes this balance effectively. It is up to individual providers to decide the level of detail provided to users. For example, we know that many providers already have community or educational pages on their service. This is also relevant to concerns raised regarding sanction circumvention addressed in chapter 3: User sanctions – Amendments to the Codes to reflect user sanctions measures.

Feedback on performance target amendments

A3.111 In response to our June 2025 Consultation, the National Center for Missing & Exploited Children (NCMEC) agreed with the proposed amendments to the performance target measures.[277] Which? stated that as performance targets are set by services, over time it expects to see industry benchmarking and providers being held to account where services do not meet the standards.[278]

A3.112 We welcome the feedback and will continue to monitor compliance with these measures, as with all our Illegal Content and Protection of Children Codes measures, as our regulatory oversight develops.

A3.113 Pinterest said that while it does not object overall to the setting of performance targets, in its experience, performance targets based solely on making decisions quickly can risk incentivising over-enforcement and deprioritising accuracy and decision quality. It said it supports a non-prescriptive outcomes-focused measure and encouraged Ofcom to amend the measure as such.[279]

Our response

A3.114 As addressed in previous statements, we consider that there are benefits to measures recommending performance targets, rather than outcomes.

A3.115 We note the risk raised by stakeholders that time related performance targets could lead to poor quality or inaccurate content moderation decisions and in turn decrease the accuracy of these decisions. However, we consider this risk is mitigated by our performance target measures that providers also set targets for the accuracy of decision-making. Providers should balance the need to take relevant content moderation action swiftly against the importance of accurate moderation decisions.

A3.116 Where providers explicitly set targets and measure performance against them, they are more likely to be able to optimise the design of their moderation functions to achieve the goals underlying the targets than they would be if they did not set targets.

A3.117 Monitoring performance against targets over time also gives providers data about how their content moderation system and processes are performing and allows them to make changes to their systems and processes to better protect users based on this data.

[277] NCMEC response to the June 2025 Consultation, p.7.
[278] Which? response to the June 2025 Consultation, p.16.
[279] Pinterest response to the June 2025 Consultation, pp.5-6.

A4. Extending user controls

Further stakeholder responses received on this chapter by theme

Requesting flexibility in applying these measures

A4.1 In their responses to the April 2025 User Controls Consultation (April 2025 Consultation), one industry stakeholder and three industry trade associations requested flexibility in applying the measures. They emphasised the need to support innovation, to consider the proportionality of the measure on specific services and argued other means may support similar objectives.[280]

Our response

A4.2 This feedback was similar to responses we received to our November 2023 Illegal Harms Consultation (November 2023 Consultation).

A4.3 As set out in paragraphs 1.33 to 1.56 and 12.47 to 12.52 of our December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement), we are required to have regard to several principles when setting our Codes of Practice (Codes).[281] The measures contained must be sufficiently clear, and at a sufficiently detailed level, that providers understand what those measures entail in practice, and that the measures for each kind and size of service must be proportionate to our assessment of the risk of harm they present.

A4.4 We also explained in the outlined paragraphs our awareness that there are many ways to design a measure. Some of these focus more on outcomes, some are more prescriptive, and some are high-level.

A4.5 Our decisions for each measure flow from the principles outlined in paragraph A1.3, our evidence base, and the results of our impact assessments. Although we acknowledge that many providers already offer similar functionalities on their services, our current evidence leads us to conclude that these measures are the most effective and proportionate way to tackle the harms identified.

A4.6 Consistent with the principles that the Codes must follow, we consider them to strike the right balance as regards to clarity and detail. As explained in the section 'Who this measure applies to' in chapter 4: Extending user controls, we consider them to be proportionate for the different types and sizes of services to which they apply, and proportionate to the risk of harm presented by those services. We set out the evidence relating to the effectiveness of these measures in the section titled: Effectiveness and benefits in chapter 4.

A4.7 The Online Safety Act 2023 (the Act) provides flexibility for providers that do not wish to adopt these measures. They may adopt alternative measures to meet their duties. As set out in the December 2024 Statement (volume 3: chapter 3: 'Ofcom's enforcement powers' and our 'Record-Keeping and Review Guidance'), providers who wish to take alternative

[280] Google LLC response to the April 2025 User Controls Consultation (April 2025 Consultation), p.1; Online Dating and Discovery Association (ODDA) response to the April 2025 Consultation, p.1; techUK response to the April 2025 Consultation, pp.2-3; [✂].

[281] Schedule 4 of the Online Safety Act 2023 (the Act).

measures may do so as long as they record how this complies with the illegal content safety duties and their duties in relation to freedom of expression and privacy.[282]

Highly effective age assurance in relation to these measures

A4.8 Parent Zone raised a concern about the language used around highly effective age assurance, querying whether it could leave open the possibility of children being left unprotected.[283]

Our response

A4.9 Our proposals to extend the application of the measures to those services listed in paragraph 4.67 in chapter 4: Extending user controls follow the same principle as in the equivalent measures in the Protection of Children Code of Practice for user-to-user services (Protection of Children Code) – that to ensure these features are offered to children, these measures should apply to all UK users who have not been determined to be adults through the use of highly effective age assurance. If a provider does not use highly effective age assurance, it would then need to offer the measures to all users on the child-accessible parts of the service.

A4.10 Providers should therefore implement these measures using one of the following approaches:

i) use highly effective age assurance to offer the measures to users who have not been determined to be adults using highly effective age assurance; or
ii) offer the measures to all users on child-accessible parts of the service.

A4.11 The provider of a service likely to be accessed by children will be in scope of both the Protection of Children Code and these measures in the Illegal Content Codes (if they meet the size, risk, and functionality criteria for both).

A4.12 Children should therefore be protected from content that is harmful to them under the Protection of Children Code, as well as being offered the option to seek further protection through the use of the blocking, muting and disabling comment tools recommended here.

Importance of accessible information for the tools

A4.13 Parent Zone reported that user controls can be confusing and inconsistent across services, citing its own research into parental controls and user empowerment showing 121 different tools across eight services. It also explained that tools have different names across platforms, may be labelled the same but function differently or change on the same service over time. It stated that these limitations should be explained to parents to prevent complacency. It called for user controls to be consistent across services and welcomed focus on comprehensibility, but expressed doubt that smaller services would comply, citing frequent use of dense language, dark pattern design and obfuscation of problematic features.[284] It quoted Ofcom research to explain that children's awareness of tools is low and that they often need more motivation to engage with tools in the first instance.[285]

[282] Section 23(4) and (5) of the Act.
[283] Parent Zone response to the April 2025 Consultation, pp.5-6.
[284] Parent Zone response to the April 2025 Consultation, pp.3-4.
[285] Parent Zone response to the April 2025 Consultation, p.3.

Our response

A4.14 In our December 2024 Statement, we explained that we recommended that providers provide information to United Kingdom users about:

a) the availability of the options to block and mute other users and the effect of these actions, including the types of interactions or access to content that it would restrict; and

A4.15 the availability of the option to prevent other users of the service from commenting on content posted on the service by the United Kingdom user concerned, and the effect of this action, including the types of interactions or access to content that it would restrict.[286]

A4.16 That information should be:

a) easy to find; and

b) comprehensible based on the likely reading age of the youngest individual permitted to use the service without the consent of a parent or guardian.

A4.17 We explained that approaches to accessibility vary from service to service, subject to their service's features and design, and on that basis took the view that providers are best placed to decide how to ensure information is accessible.

A4.18 However, providers should consider their obligations under other relevant legislation (for example, the Equality Act 2010) and, where relevant, appropriate guidance. We have not been prescriptive about the language in which service providers should give information to users regarding these features. We expect service providers would determine which language(s) would best suit their userbase.

Emerging technologies and these measures

A4.19 VoiceBox and Parent Zone requested further information on how these measures would apply to emerging technologies including virtual reality (VR), XR (extended reality), AI-enabling wearables, and picture-based forums. They provided examples and cited third-party research demonstrating the harm that users, and specifically children, can experience through such means.[287]

Our response

A4.20 "Content" as defined by the Act means anything communicated by means of an internet service, whether publicly or privately, including written material, or messages, oral communications, photographs, videos, visual images, music and data of any description.[288]

A4.21 Our Codes are designed with this definition in mind to be content, technology and service agnostic, ensuring applicability across a wide range of service types and functionalities. The measures presented in chapter 4: Extending user controls rely on the definition of "content" in the Act.[289]

---

[286] Ofcom (2024), December 2024 Statement, Vol.2, chapter 12: User Controls.
[287] Parent Zone response to the April 2025 Consultation, p.4.; VoiceBox response to the April 2025 Consultation, p.4.
[288] As defined in annex 6: Glossary.
[289] The blocking and muting measures apply to services that have "posting content functionality", which is defined as a "user-to-user service functionality allowing users to do one or more of generating, uploading or sharing content on open channels of communication". The measures also affect blocking/muting users' ability to encounter "content posted" by blocked/muted users, which is defined in Section 5 of the Codes as "content

A4.22 We recognise that emerging technologies such as extended reality are still in the early stages of development and adoption, and that the services built on them, the content they offer, as well as their safety features are continuing to evolve. We will keep this under review.

Safety by design and placing the onus of safety on the individual

A4.23 Several civil society and the Scottish Government emphasised the importance of providers implementing safety by design to ensure the onus is not primarily on children to keep themselves safe.[290] The Scottish Government and the Antisemitism Policy Trust cautioned that controls like blocking and muting are helpful but insufficient if users are unaware of them or reluctant to use them.[291]

A4.24 The Scottish Government also stated that user controls must not absolve services from actively removing illegal content.[292] Parent Zone warned that poorly designed tools could undermine safety rather than improve it, and stressed the importance of thoughtful implementation.[293] The Antisemitism Policy Trust said that safety settings for young users should be on the highest level by default and stressed the need for stronger moderation tools to prevent exposure to antisemitic content without relying on users having to proactively block it.[294]

Our response

A4.25 This is similar to the feedback we received in response to the November 2023 Consultation and our May 2024 Consultation on Protecting Children from Harms Online (May 2024 Consultation). The Antisemitism Policy Trust also suggested that safety settings for young users should be on the highest level by default.[295]

A4.26 As explained in our December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement) and April 2025 Statement on Protecting Children from Harms Online (April 2025 Statement), we agree with this feedback, which is why we have a diverse suite of measures. Some of these measures place an expectation for proactive action on service providers, while others provide users with options for protecting themselves from harmful content and making safer choices.[296] As part of these measures,

---

generated, uploaded and/or shared on open channels of communication by a user of the service". The disabling comments measure prevents users from being able to "comment on content", which is defined in Section 5 of the Codes as being able to "reply to user-generated content, or generate, upload or share content in response to another piece of user-generated content posted on open channels of communication, in such a way that the reply or content (as the case may be) is visually accessible directly from the original user-generated content without navigating away from that user-generated content".

[290] 5Rights Foundation response to the April 2025 Consultation, pp.2-3; Antisemitism Policy Trust response to the April 2025 Consultation, p.4.; Scottish Government response to the April 2025 Consultation, p.2.

[291] Antisemitism Policy Trust response to the April 2025 Consultation, p.4.; Scottish Government response to the April 2025 Consultation, p.2.

[292] Scottish Government response to the April 2025 Consultation, p.2.

[293] Parent Zone response to the April 2025 Consultation, p.3.

[294] Antisemitism Policy Trust response to the April 2025 Consultation, pp.4-5.

[295] Antisemitism Policy Trust response to the April 2025 Consultation, p.4.

[296] As explained in the section 'Introduction' of chapter 12: User controls in the December 2024 Statement, this is in line with the Act, which expressly refers to "functionalities allowing users to control the content they encounter" as an area in which providers must take measures, if proportionate, to comply with their illegal content safety duties. For example, measure ICU F1 recommends that providers should implement safety defaults for child user accounts, which target particular functionalities and that restrict the visibility and

and as we clarify that information should be provided to users on the availability of the options to block, mute and disable comments and that this information should be a) easy to find; and b) comprehensible based on the likely reading age of the youngest individual permitted to use the service without the consent of a parent or guardian. These measures should therefore help both adult and child users in making safer choices.

A4.27 Even in the context of safer online environments, it is important for children to have control over the users and content they encounter, to make informed and effective use of online safety tools, and to be able to access support when they need it. This reflects feedback from our engagement with children that while responsibility for keeping children safe should sit with service providers, they do value control over their online experience.[297] These measures are intended to give children this control within the context of safer online services, by providing them with the tools and information to navigate services in a safe and supportive way.

Assessment of risk levels and children's access

A4.28 Multiple stakeholders requested further specific information on how providers would assess risk level or children's access to their services:

A4.29 Parent Zone asked what a service at medium risk of encouraging or assisting suicide looked like.[298]

A4.30 The Antisemitism Policy Trust requested specific interpretations of high and medium risk in the context of antisemitism.[299]

A4.31 C3P expressed concern over how providers will assess their services as being likely to be accessed by children.[300]

A4.32 The Antisemitism Policy Trust suggested that all services that are widely used by children should be considered medium risk.[301]

Our response

A4.33 Our risk assessment guidance suggests a range of evidence that can be used to determine levels of risk for different illegal harms such as the encouragement of suicide or hate. A small pro-suicide forum would have significant risk factors, which would likely lead it to be assessed as high risk rather than medium risk. Our risk assessment guidance also defines hate in the context of religiously aggravated offences as per the Public Order Act 1986.

A4.34 We have published guidance to help providers establish whether their service is likely to be accessed by children and we may consider taking enforcement action if we consider that a service has failed to carry out a suitable and sufficient assessment.

---

engagement between child users and other users; measure ICU F2 recommends that providers should give child users relevant supportive information at critical points in a child user's journey to allow child users to make more informed choices. Providers should ensure the messaging is prominently displayed and is clear and easy for children to understand.

[297] Ofcom (2025), Consulting children on Protection of Children Online Safety Proposals.

[298] Parent Zone response to the April 2025 Consultation, p.5.

[299] Antisemitism Policy Trust response to the April 2025 Consultation, p.4.

[300] C3P response to the April 2025 Consultation, pp.2-3.

[301] Antisemitism Policy Trust response to the April 2025 Consultation, p.5.

A4.35 Providers must assess the risk of their services based on the matters set out in the Act (in sections 9(5) and 26(5)). The fact that a service is widely used by children is a contributor to the likelihood and impact of harm and will form part of a wider risk assessment.

Recommending measures based on service size and risk

A4.36 C3P said a threshold of child users should be used to determine which services are in scope and that threshold should be lower than 700,000. It also highlighted a number of services with fewer than 700,000 users which present risks to children.[302]

A4.37 5Rights Foundation and VoiceBox said measures should be recommended to services based solely on risk and not size.[303]

Our response

A4.38 We use total monthly UK users, including adults, in our definition of size. We do not use a separate threshold for children in the definition because this definition is partly intended as a proxy for the resources a service provider may have, and because without the use of highly effective age assurance providers may not know their number of child users.[304] We recognise that there are some services that are likely to be used disproportionately by children, and this forms part of our reasoning for extending the application of the measures to smaller services.

A4.39 The Act requires us to ensure regulation is proportionate to the size or capacity of the provider when recommending measures, and we have taken this into account in our approach to this measure.

Uncertainty for users on which services provide user controls

A4.40 Parent Zone warned that categorising services by size could have unintended consequences where it is unclear to parents which services have the safety tools and children could migrate to smaller and less-regulated services.[305]

Our response

A4.41 While parents will not know how many users a service has, the measures we are recommending are that all services that are likely to be accessed by children and high risk of the relevant harms should have the user controls regardless of their number of users. In addition, we have recommended that those in scope of the measures provide information about the tools that is easy to find. Parents will be able to see on a service-by-service basis what safety tools are available to users. If children migrate to other, possibly smaller, services then these other services will gain users over time. They may then reach the size at which they will be in scope of these measures, in addition to other measures.

---

[302] C3P response to the April 2025 Consultation, pp.4-5.
[303] 5Rights Foundation response to the April 2025 Consultation, pp.1-2; VoiceBox response to the April 2025 Consultation, p.2.
[304] We do this consistently across our Codes of Practice. See paragraphs 1.160 to 1.165 in 'Our approach to developing Codes measures' in the December 2024 Statement.
[305] Parent Zone response to the April 2025 Consultation, p.5.

Request for stronger moderation and enforcement

A4.42 A number of stakeholders requested improved moderation on services and noted service providers' failure to respond to user reports. Others asked questions around compliance and enforcement, and said our interpretation of the Act is too industry-focused:

a) The Antisemitism Policy Trust warned that weakened moderation by major platforms and poor age verification are exposing children to harmful content, and called for regulation to set minimum standards and ensure AI moderation tools are properly trained to detect antisemitism and other hate speech.[306]
b) The Antisemitism Policy Trust also stated that the continued prevalence of antisemitism online across all services, including illegal content, suggests a lack of urgency by providers to comply with their duties under the Act.[307]
c) VoiceBox questioned the effectiveness of blocking and muting tools alone, urging us to consider complementary measures like proactive moderation and systemic design changes.[308]
d) VoiceBox cited youth frustration at the lack of follow-up from services on reports, which could deter children from using the tools and calls for better moderation of responses.[309]
e) The Antisemitism Policy Trust warned that proposals to protect children may fall short without stronger age verification, improved moderation, increased safety-by-design, and consistent enforcement. It also expressed concern that our interpretation of the Act may be overly influenced by tech companies' financial interests.[310]
f) VoiceBox asked for additional information on how we planned to enforce the measures, warning that without robust mechanisms for oversight, some service providers may only superficially comply or fail to respond to user reports.[311]

Our response

Improved moderation on services

A4.43 Regarding feedback on the need for improved moderation on services, the Protection of Children and Illegal Content Codes contain several measures that aim to ensure providers take down illegal content and content harmful to children swiftly.

A4.44 This includes having a content moderation function that allows for the swift take down of illegal harms and primary priority content/priority content harmful to children, setting internal content policies, setting performance targets for its content moderation function, and applying a policy in respect of the prioritisation of content.[312]

A4.45 In the December 2024 Statement we explained in detail how we expect these moderation measures to be effective in ensuring providers comply with their duties to protect users from illegal content and children from harmful content. It is up to service providers to

[306] Antisemitism Policy Trust response to the April 2025 Consultation, p.4.
[307] Antisemitism Policy Trust response to the April 2025 Consultation, pp.5-6.
[308] VoiceBox response to the April 2025 Consultation, p.4.
[309] VoiceBox response to the April 2025 Consultation, pp.3-4.
[310] Antisemitism Policy Trust response to the April 2025 Consultation, p.4.
[311] VoiceBox response to the April 2025 Consultation, p.3.
[312] Protection of Children Codes of Practice for user-to-user-services (Protection of Children Codes), Measures PCU C2-C5; Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes), Measures ICU C2-C5.

decide whether they go beyond the recommendations in the Codes to improve their moderation functions, as long as they comply with the safety duties outlined in the Act.

Failure to respond to user reports

A4.46 The Protection of Children and Illegal Content Codes contain several measures that aim to ensure providers have robust reporting and complaints systems in place. These include measures for providers to acknowledge receipt of a complaint, to provide complainants with an indicative timeframe for when a complaint might be resolved, and to take appropriate action in relation to each type of relevant complaint.[313]

Compliance and enforcement

A4.47 In response to VoiceBox's question on how we plan to enforce the measures against providers of small services, as part of our role as the independent regulator for online safety in the UK, we may take enforcement action where it is in the interests of citizens and consumers to promote compliance, deter future wrongdoing, protect users from harm, and hold wrongdoing to account. The Communications Act 2003 requires us to have regard, in all cases, to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent, and targeted only in cases in which action is needed, and any other principles appearing to represent the best regulatory practice.[314] In terms of enforcement, this means we will take action where it is proportionate and appropriate, but with a willingness to intervene firmly, promptly and effectively when required. We will always seek the least intrusive regulatory methods to achieve our objectives and ensure that interventions are evidence-based, proportionate, consistent, accountable, and transparent in both deliberation and outcome, in line with our regulatory principles.

A4.48 The Online Safety Enforcement Guidance sets out how we will normally approach enforcement under the Act.[315] The approach set out in this guidance has been informed by our experience and track record of enforcement in other sectors that we regulate.

Ofcom's interpretation of the Act being too industry-focused

A4.49 In our December 2024 Statement, we explained our approach to developing the Codes in detail.

A4.50 When assessing the case for including a measure in the Codes, we considered the following factors:

a) the prevalence and impact of the harm the measure is combatting;

b) the efficacy of the measure in combatting this harm;

c) the direct and indirect costs of the measure;

d) the impact the measure would have on privacy and freedom of expression; and

e) any risks associated with the measure.

A4.51 We weighed these factors against one another to assess whether the measure in question would be proportionate when seen in the round. As part of this assessment, we considered whether it would be proportionate to apply the measure to all services or a subset of services. We also considered both the individual and cumulative impact of the measures.

---

[313] Protection of Children Codes, Measures PCU D4-D5; Illegal Content Codes, Measures ICU D4-D5.
[314] Section 3(3) of the Communications Act 2003.
[315] Ofcom (2024), Online Safety Enforcement Guidance.

A4.52 We have considered the impact on providers to ensure that the likely costs associated with each measure are justified. This is partly because imposing costs on providers can have negative impacts or risks for users. For example, if an increased cost burden on providers reduced investment in areas other than user safety or drove some services to stop operating in the UK, this could mean that users no longer benefitted from such services or new innovations, and could be detrimental to the UK's economic growth.[316] We are also required under the Act to consider the proportionality of measures having regard to the size and capacity of the provider, and to carry out an impact assessment.

A4.53 This does not mean that a measure is necessarily disproportionate because it imposes significant costs on providers or because it creates risk of some services ceasing to operate in the UK. While there may be a loss to users from some services ceasing to operate, this may be in users' overall interests if such services are causing significant harm through illegal content and if providers are not prepared (or cannot afford) to apply a measure to sufficiently address that harm.

Preventing harmful contact

A4.54 A number of stakeholders either suggested new measures, or suggested measures where we have something similar in place already:

A4.55 The Antisemitism Policy Trust said the measures should include options for children to block or filter anonymous users, noting that antisemitic content frequently comes from untraceable accounts and poses a heightened risk of exposure to hate speech.[317]

A4.56 VoiceBox advocated for mandatory user accounts on small but harmful services followed by the suggested proposals, citing risks from livestreaming services which allow for adult content to be pushed and seen without an account.[318]

a) In addition to global blocking, C3P stressed the importance of preventing people making fake accounts and preventing unsolicited contact from strangers to teens in the first place.[319]

A4.57 C3P said that blocking and muting are important but must be complemented to prevent recontact from new accounts, citing research showing that teens are often reapproached after blocking, and recommends device or network-level blocking for more robust protection.[320]

Our response

A4.58 We note the comments from the Antisemitism Policy Trust. In order for a tool that filters anonymous users to be effective, it would need to be recommended alongside a measure on identity verification; if users had no way of verifying themselves then the tool would filter out all users. We explained in the Illegal Harms Statement that we were not recommending mandatory identity verification.[321] As part of annex 10 of our Additional Duties Consultation, we also explained that we are currently of the view that the available evidence does not support the consideration of an optional identity verification measure in

[316] We are required under section 108 of the Deregulation Act 2015 to have regard to the desirability of promoting economic growth when carrying out our functions.
[317] Antisemitism Policy Trust response to the April 2025 Consultation, p.4.
[318] VoiceBox response to the April 2025 Consultation, p.4.
[319] C3P response to the April 2025 Consultation, p.2.
[320] C3P response to the April 2025 Consultation, p.2.
[321] Ofcom (2024), December 2024 Statement, Vol.2, chapter 11: User Access.

the Illegal Content Codes. As such, we do not currently consider there to be a case for adopting a measure of this nature, though we will continue to monitor evidence in this area. In the meantime, we consider the blocking (in particular global blocking) and muting measures will enable users to protect themselves from illegal content from anonymous accounts.

A4.59 VoiceBox and C3P requested additional measures. We consider that the decisions in this statement will ensure a significantly safer environment online for all users, in particular children. We will be closely monitoring how service providers implement the measures in the Codes, as well as the wider package of protections for children. We will also consider whether any future legislative changes require updates to our current position and will consult before making any such changes as appropriate

A4.60 In response to C3P's point about preventing unsolicited contact from strangers, we have a suite of measures proposed in the Illegal Content Codes for this purpose. We consider these measures to be effective in blocking unsolicited contact from adults to children.[322] We also expect that being able to block all unconnected users will go some way to address C3P's concerns.

Request for additional guidance

A4.61 Stakeholders also suggested additional guidance that they considered would be beneficial:

a) The Antisemitism Policy Trust urged us to prepare targeted resources for very small platforms popular with children which may have limited resources for moderation and age assurance, stating this was needed to prevent exploitation by extremists and improve safety against hate speech and antisemitism.[323]
b) techUK highlighted that age assurance is foundational for enabling these measures and recommended that we signpost proportionate, privacy-respecting age assurance options and methods to support affordable compliance, particularly for smaller platforms. It said these examples should consider the range of age assurance options for different use cases, spanning age verification, age estimation, and age inference.[324]
c) Parent Zone argued that adult-designed user controls are unlikely to protect children without added support. It recommended we include additional requirements or "best practice" for services to include follow-up mechanisms and signposting, citing its own "digital pattern library" as a model.[325]
d) VoiceBox also recommended scaled-down transparency reports on small but harmful services to provide us with greater visibility into user safety.[326]

Our response

A4.62 In response to the Antisemitism Policy Trust, we are required by the Act to provide guidance on the types of content that we consider to be harmful to children and guidance

[322] Measure ICU F1 recommends that providers should implement safety defaults for child user accounts, which target particular functionalities and that restrict the visibility and engagement between child users and other users; measure ICU F2 recommends that providers should give child users relevant supportive information at critical points in a child user's journey to allow child users to make more informed choices. Providers should ensure the messaging is prominently displayed and is clear and easy for children to understand.
[323] Antisemitism Policy Trust response to the April 2025 Consultation, p.5.
[324] techUK response to the April 2025 Consultation, pp.2-3.
[325] Parent Zone response to the April 2025 Consultation, pp.2-3.
[326] VoiceBox response to the April 2025 Consultation, p.4.

to support service providers in understanding their regulatory obligations when making judgments about whether content is illegal. Service providers can refer to these when considering their moderation processes.[327]

A4.63 In response to [✂], we have also provided guidance on highly effective age assurance to which providers can refer.[328]

A4.64 In response to Parent Zone, we give providers flexibility in how to implement the measures in a way that works for their services which includes how the tools are designed and presented.

A4.65 VoiceBox's request for scaled-down transparency reports goes beyond the remit of the Act and is not something we would be able to implement.

Tech literacy and parental support

A4.66 Stakeholders offered a number of suggestions on how to improve a child's tech literacy, or to make parental support official:

a) Internet Matters supported Ofcom's proposal for clear guidance on user controls, highlighting gaps in children's awareness across services and encourage service providers to go beyond the Codes and embed media literacy by design to improve understanding and usage.[329]
b) Internet Matters urged Ofcom to formalise parents' role in the Illegal Content Codes and called on service providers to better support them. This could include providing accessible guidance to parents on user controls without requiring a personal account.[330]
c) 5Rights Foundation called for user control features like blocking and muting to be tailored to children's needs, urging service providers to support children both after they block others and when they are blocked, and to prevent them from bypassing safeguards by creating adult accounts.[331]
d) Parent Zone noted that children may be overconfident in their abilities to deal with harm online or may avoid using user controls due to fear of retaliation or reduced enjoyment. It warned that this could leave them unprotected and give parents a false sense of safety despite the user experience not being safe.[332]

Our response

A4.67 In response to Internet Matters' first point, we agree that this could be beneficial for users. It is for providers to decide to go beyond the Codes if they wish to do so.

A4.68 In response to Internet Matters' second point, our Protection of Children Code includes measures to this effect. PCU F1 and PCS F4 recommend providers of services in scope of this measure develop age-appropriate user support materials for children, including explanations for the adults who care for them, ensuring that children can understand the user support tools and reporting and complaints functions on the service, and how to use these to mitigate the risk and impact of encountering harmful content.

---

[327] Ofcom (2025), Protecting Children from Harms Online: Guidance on Content Harmful to Children; Ofcom (2024), Illegal Content Judgements Guidance.
[328] Ofcom (2025), Guidance on highly effective age assurance and other Part 5 duties.
[329] Internet Matters response to the April 2025 Consultation, p.1.
[330] Internet Matters response to the April 2025 Consultation, pp.3-4.
[331] 5Rights Foundation response to the April 2025 Consultation, p.2.
[332] Parent Zone response to the April 2025 Consultation, p.2.

A4.69 5Rights Foundation requested a measure that we have already recommended. Our Illegal Content Codes for user-to-user services already includes a measure recommending support to children where they block a user (ICU F2).

A4.70 In response to Parent Zone's comment on children's abilities to use user controls, we have a diverse suite of measures. Some of these measures place an expectation for proactive action on service providers, while others provide users with options for protecting themselves from harmful content and making safer choices.

A4.71 Even in the context of safer online environments, it is important for children to have control over the users and content they encounter, to make informed and effective use of online safety tools, and to be able to access support when they need it.

A5. Highly effective age assurance in the Illegal Content Codes

Further stakeholder responses received for our measure on introducing highly effective age assurance to the Illegal Content Codes by theme

Highly effective age assurance will restrict adults' access to services

A5.1 Individual respondents and digital-rights groups warned that expanding highly effective age assurance could risk excluding adults who are unwilling to share their personal data by wrongly treating them as children. They argued that mandatory age checks for adults would be disproportionate and incompatible with a free society.[333]

Our response

A5.2 We note that the expansion of highly effective age assurance to more services and contexts may deter adults from using a service. However, the form of highly effective age assurance used is subject to the service provider, and they should consider their user base when making such decisions. Given adults will still have access to services if they undergo highly effective age assurance, and the importance of highly effective age assurance in providing adequate protections for children online, we consider these measures to be proportionate.

Highly effective age assurance could restrict children's access to beneficial content

A5.3 The Online Safety Network (OS Network) warned that applying highly effective age assurance uniformly to all users could reduce providers' ability to identify children and deliver age-appropriate messaging, interventions or support, including in contexts where children may be at risk of grooming. They suggested a hybrid approach comprising a baseline level of highly effective age assurance across services, supplemented by additional protective measures in higher-risk settings, such as livestreaming, together with prioritised support pathways for children.[334]

A5.4 An individual respondent raised concerns that age assurance and moderation measures could inadvertently limit children's access to lawful, educational, informational and support content online, including resources that children may rely on for learning, advice or support.[335]

---

[333] British and Irish Law Education Technology Association (BILETA) response to the June 2025 Consultation, p.34; Klaushofer, A. response to the June 2025 Consultation, p.9; Name Withheld 26 response to the June 2025 Consultation, p.9.
[334] Online Safety Network (OS Network) response to the June 2025 Consultation, pp.24-25.
[335] [✂].

Our response

A5.5 We recognise that access to educational, informational and support content can be important for children. Our approach to highly effective age assurance is not intended to prevent children from accessing lawful content, but to enable child-specific protections to be applied where appropriate.

A5.6 Highly effective age assurance should support the accurate targeting of safety measures, rather than to impose blanket restrictions on access. Providers retain flexibility in how they design and implement protections, including through service design, settings and safeguards that reduce harm while preserving access to beneficial content. Where age assurance measures result in an incorrect assessment that affects a user's experience, the appeals mechanisms set out in this statement provide a route for redress. We therefore consider that the measures strike an appropriate balance between reducing risks to children and maintaining access to lawful educational and support resources.

Highly effective age assurance should be applied in further contexts

A5.7 The National Police Chiefs' Council (NPCC) said highly effective age assurance could ease pressure on child sexual abuse (CSA) referral systems by raising barriers to offending, while UK Finance argued the definition should also address fraud risks affecting children, older adults, and vulnerable groups, recommending a data-driven approach that incorporates financial-crime prevention.[336]

Our response

A5.8 We take note of the suggested benefits of applying highly effective age assurance to tackle further harms. However, we consider the current measures to be proportionate and balanced to address the relevant harms at present. As such, we note these suggestions but are not actioning them at this time.

The highly effective age assurance requirement for virtual reality should be clarified

A5.9 The Institution of Engineering and Technology (IET) warned that immersive technologies, – – especially virtual reality (VR) – present major age assurance and safety gaps, with research showing rapidly growing child use and frequent exposure to abuse, exploitation, and harmful content. It urged clearer regulatory responsibilities and stronger safeguards, arguing that VR's immersive, avatar-based interactions heighten risks and that current age limits are poorly enforced.[337]

Our response

A5.10 We acknowledge the specific harms to children linked to VR and the evidence provided. We note that these use cases are not exempt from the Online Safety Act 2023 (the Act), and VR services must ensure that children benefit from the same protections in their apps and websites as they would in other online services.

---

[336] National Police Chiefs' Council (NPCC) response to the June 2025 Consultation, p.13; UK Finance response to the June 2025 Consultation, p.15.

[337] Institution of Engineering and Technology (IET) response to the June 2025 Consultation, pp.1-2.

Highly effective age assurance should be less prescriptive

A5.11 A range of respondents including industry associations and individuals urged Ofcom to allow flexible, outcome-based age-assurance approaches, arguing that mandatory highly effective systems are often disproportionate, intrusive, and duplicative – especially for gaming and mid-sized services that already use strong safety-by-design tools. Several contributors advocated privacy-preserving methods such as 'zero-knowledge age tokens' and warned that rigid requirements could create user friction, high costs, and practical implementation challenges.[338]

Our response

A5.12 As detailed in our January 2025 Age Assurance and Children's Access Statement (January 2025 Statement), we have considered proportionality in developing our approach to highly effective age assurance. This includes giving service providers flexibility in implementing a highly effective age assurance process which is suitable for their service and user base. Where existing measures comply with highly effective age assurance criteria, they do not need to be duplicated.

Highly effective age assurance should be more accessible

A5.13 The Computer & Communications Industry Association (CCIA), Cetatea Viitorului, and the British and Irish Law Education Technology Association (BILETA) all highlighted accessibility concerns, stressing that highly effective age assurance must work for users who cannot easily prove their age, including those with low digital literacy or additional needs. They called for more adaptable methods such as SMS-based checks, multilingual parental-control guidance, and stronger safeguards around third-party providers.[339]

Our response

A5.14 We are clear in the draft Guidance on Highly Effective Age Assurance for Part 3 Services (Part 3 HEAA Guidance) that accessibility is an additional principle we expect service providers to consider, with a view to ensuring that adults are not unduly prevented from accessing legal content and that children are prevented from encountering content which is harmful to them. We expect services to consider accessibility not only in the context of specific methods, but across the entire age assurance process they implement. While any single method may not be accessible to all users, this can be mitigated where services offer alternative methods as part of a broader, accessible age assurance process. In line with our principles, age assurance should also be easy to use and work effectively for all users, regardless of their characteristics.

Highly effective age assurance should be supported by ID verification

A5.15 Law enforcement and financial crime prevention bodies said that highly effective age assurance alone is insufficient, urging stronger identity verification to prevent

[338] [✂]; Computer & Communications Industry Association (CCIA) response to the June 2025 Consultation, p.14; Edwards, L. response to the June 2025 Consultation, p.9; [✂]; [✂].
[339] BILETA response to the June 2025 Consultation, p.32; CCIA response to the June 2025 Consultation, p.14; Cetatea Viitorului response to the June 2025 Consultation, p.2.

impersonation, reregistration, and fraud; they noted that youth offending rates and inaccuracies in age-only checks make complementary identity assurance essential.[340]

Our response

A5.16 In our Part 3 HEAA Guidance, we explain what we consider to be highly effective technologies – digital identity solutions can fall into this category. As set out in Ofcom's Part 3 HEAA Guidance, our remit for highly effective age assurance is limited to determining whether users are over 18 in a privacy-preserving way, not verifying their identity.[341]

A5.17 It is therefore important to distinguish between the use of ID-based methods to derive an age attribute, and full identity verification, which involves establishing who a user is. Full identity verification goes beyond what is recommended for age assurance under these measures, and we are not introducing identity verification requirements.

Highly effective age assurance needs minimum accuracy thresholds

A5.18 Three stakeholders urged us to define "highly effective" age assurance through strict, enforceable technical standards and measurable performance thresholds, with mandatory certification, transparency, and support for privacy-preserving age tokens.[342]

A5.19 The National Society for the Prevention of Cruelty to Children (NSPCC) and several others supported accessible, accurate appeals but warned that most appeals would be from adults wrongly classified as children, risking incentives to overestimate ages unless minimum accuracy standards – such as a 95% benchmark – are set.[343] Along with NetChoice, the OS Network, and individual respondents, they emphasised the need for clear safeguards, timelines and redress, while others cautioned that flawed assessments could restrict lawful adult access and undermine trust.[344]

Our response

A5.20 We consider that there is more to ensuring an approach is "highly effective" than simply citing a third-party provider's accuracy score. Our intention is to encourage providers to take a broader, criteria-based approach, which we consider secures the best outcomes for ensuring the protection of children online. We consider that effectiveness can be demonstrated in ways other than specifying a single numerical accuracy threshold.

A5.21 We also recognise that accuracy thresholds may play a role as the evidence base and industry standards continue to develop, and that thresholds could in future complement our criteria-based framework. At present, we consider that there is insufficient evidence or consensus to define an appropriate threshold, and that setting one prematurely could create unintended outcomes on ensuring children are protected from harmful content

---

[340] Department of Justice for Northern Ireland response to the June 2025 Consultation, p.16; [✂]; NPCC response to the June 2025 Consultation, p.13; UK Finance response to the June 2025 Consultation, pp.14-15.
[341] Ofcom (2025), Guidance on highly effective age assurance.
[342] 5Rights Foundation response to the June 2025 Consultation, p.14; Barnardo's response to the June 2025 Consultation, p.18; [✂].
[343] [✂]; National Society for the Prevention of Cruelty to Children (NSPCC) response to the June 2025 Consultation, p.47.
[344] [✂]; [✂]; Harris, B. response to the June 2025 Consultation, p.7; Name Withheld 9 response to the June 2025 Consultation, p.9; NetChoice response to the June 2025 Consultation, pp.3-4; OS Network response to the June 2025 Consultation, pp.25-26.

online. We are actively monitoring and engaging in this fast-moving space at a UK and international level, and we expect to return to this question in future.

Highly effective age assurance could negatively impact the rights of adults online

A5.22 Three individual respondents, along with NetChoice, argued that the expansion of highly effective age assurance risks over-blocking lawful content, undermining adults' freedom of expression and privacy, and creating disproportionate barriers for legitimate adult users, warning that automated systems could censor or delay access and entrench an unnecessary verification infrastructure.[345]

Our response

A5.23 We have addressed the impact of highly effective age assurance on freedom of expression and privacy where it restricts access to services, content, and limits user experiences in our January 2025 Statement and our April 2025 Statement on Protecting Children from Harms Online (April 2025 Statement).

A5.24 Any delays to the adult user experienced caused by highly effective age assurance is proportionate to the outcomes we are aiming to achieve. The degree of interference with a user's experience is subject to the form of highly effective age assurance adopted by a provider.

Highly effective age assurance should be used to differentiate age groups

A5.25 The OS Network noted Ofcom had not addressed differences between age groups of children and said services should introduce measures tailored to different ages if they know users' ages.[346]

Our response

A5.26 Introducing age verification or mandatory age-band differentiation goes beyond the scope of highly effective age assurance. Highly effective age assurance establishes a strong baseline of protection for all children. Consistent with Ofcom's Part 3 HEAA Guidance, providers retain flexibility to design and implement age assurance processes that are appropriate for their services and may choose to use age-related information, including age ranges, to tailor protections for different groups of children where appropriate.[347]

[345] [✂]; Harris, B response to the June 2025 Consultation, p.7; Name Withheld 9 response to the June 2025 Consultation, p.9; NetChoice response to the June 2025 Consultation, pp.3-4.
[346] OS Network response to the June 2025 Consultation, p.9.
[347] Ofcom (2025), Guidance on highly effective age assurance.

Further stakeholder responses received on our measure on introducing age assessment appeals by theme

Propositions to expand or alter appeal measure

A5.27 A number of respondents highlighted the need for fair, timely, and secure appeals processes for age-assessment errors, with safeguards against fraud, options for users to submit evidence, and tools like standardised reporting categories and safety-by-design defaults; however, some individuals argued appeals were unnecessary and that users should decide content suitability themselves.[348] One respondent said that some service providers' existing mechanisms could meet regulatory expectations and should not be required to duplicate them.[349]

Our response

A5.28 Our guidance is designed to provide services with the flexibility to choose an appeals approach that best fits their user base, operational model, and the technologies they use. This flexibility allows providers to adopt proportionate processes while still meeting their regulatory duties. However, an appeals mechanism must not weaken or circumvent a highly effective age assurance method. Any approach that compromises the integrity of the system would undermine its effectiveness and is therefore not recommended.

A5.29 Within this approach, services may incorporate additional safeguards or supporting features where appropriate, such as mechanisms for users to provide further evidence, clear routes for reporting incorrect age assessments, timely handling of appeals, or measures to prevent fraudulent attempts to bypass restrictions. These are compatible with our approach provided they reinforce – rather than dilute – the security, privacy, and reliability of the age-assurance method deployed.

Cost of appeals could diminish resources to counter fraud

A5.30 UK Finance said that increased costs of handling age assessment appeals could reduce funding for fraud prevention measures. It added that the ease of creating bot accounts could overwhelm providers when addressing these issues.[350]

Our response

A5.31 While implementing the age assessment appeals will incur some costs, these are important for the accuracy of highly effective age assurance assessments and the rights of users.

Appeals need human oversight

A5.32 Two individual respondents said it was vital for users to have a simple appeal process and access to human review within 24 hours, with one citing Yoti's white paper which showed reduced accuracy of some age assurance methods in low-light conditions.[351]

---

[348] BILETA response to the June 2025 Consultation, pp.31-32; Harris, B. response to the June 2025 Consultation, p.8; [✂]; NSPCC response to the June 2025 Consultation, p.46; [✂]; UK Finance response to the June 2025 Consultation, p.14; [✂].

[349] Association for UK Interactive Entertainment (Ukie) response to the June 2025 Consultation, p.35.

[350] UK Finance response to the June 2025 Consultation, p.15.

[351] Edwards, L. response to the June 2025 Consultation, p.7; [✂].

Our response

A5.33 As set out in our June 2025 Additional Safety Measures Consultation (June 2025 Consultation), we expect service providers to provide prompt and reliable user redress mechanisms. Human oversight can be one way to achieve this.

Further cross-cutting stakeholder responses received by theme

A5.34 We also received feedback from stakeholders on our entire highly effective age assurance approach.

Highly effective age assurance circumvention

A5.35 A number of individuals – as well as respondents across civil society, industry, government, and law enforcement – stated that virtual private networks (VPNs) undermined the measure by giving users a means to circumvent highly effective age assurance.[352] They argued that VPNs and related workarounds can undermine highly effective age assurance and pointed to reported spikes in VPN usage, free or bundled VPN options and forum guidance that make circumvention easy. They raised child safety, privacy, and law enforcement risks, and asked us to research and monitor VPN use and to clarify that methods commonly bypassed would not qualify as highly effective.

Our response

A5.36 In July 2026 we published our Use of Age Assurance Report.[353] In this, we found that circumvention of age assurance appears low, with a relatively small minority of children reporting that they circumvent highly effective age checks or use VPNs to access restricted content of features. However, some activity may not be captured due to reporting bias.

A5.37 Our evidence suggests that VPN use increased among UK users, but does not currently show that this increase is due to children motivated by a desire to bypass age checks on online services. Evidence on circumvention techniques is limited but indicates that robust configuration and monitoring of age assurance processes is important to mitigate known and emerging risks.[354] Our Part 3 HEAA Guidance is clear that services must not direct or encourage users to circumvent age assurance, including through the use of VPNs.[355]

A5.38 We will continue to monitor VPN usage and develop our evidence base on circumvention and displacement, but it would be a matter for the government to decide whether to take steps to address VPN usage by children.

[352] Barnardo's response to the June 2025 Consultation, p.17; CCIA response to the June 2025 Consultation, p.14; Name Withheld 4 response to the June 2025 Consultation, p.11; Name Withheld 26 response to the June 2025 Consultation, p.9; [✂]; NPCC response to the June 2025 Consultation, p.13; Scottish Government response to the June 2025 Consultation, p.2; Together Declaration Campaign response to the June 2025 Consultation, p.5.

[353] Ofcom (2026), Use of Age Assurance, p.4; Ofcom (2026), Children's use of VPNs.

[354] Ofcom (2026), Use of Age Assurance, p.61.

[355] Ofcom (2025), Guidance on highly effective age assurance, p.16.

Cost for smaller services

A5.39 A respondent expressed support for our assessment of costs, including for smaller services.[356] Digital Resilience in Education (Welsh Government) said that these measures had low financial costs, but they could improve trust and reputation for service providers, encouraging more user engagement and potentially increasing advertising revenue.[357]

A5.40 Stakeholders across civil society, industry and academic associations said that while protecting children from adult content is important, proposals to codify or expand highly effective age assurance risk placing disproportionate and sometimes unaffordable burdens on smaller services, particularly because of the complexity, cost, and timing of implementation.[358] They warned that a one-size-fits-all approach could reduce competition, innovation, and market diversity, and several argued that requirements such as appeals processes or applicability to smaller service providers would exacerbate these impacts. Stakeholders emphasised the need for proportionate, risk-based, and scalable measures that remain practical for small and medium enterprises, preserve privacy and user autonomy, avoid invasive data collection, and ensure that obligations align with each service's risk profile and functionality.

Our response

A5.41 In our June 2025 Consultation, we said that while providers may face some additional costs when implementing the definition, introducing an appeals mechanism, and monitoring accuracy, these are expected to be limited, with overlap across existing duties regarding appeals, as explained in chapter 5: Highly effective age assurance in the Illegal Content Codes, paragraph 5.85. These costs are outweighed by the benefits of greater consistency in our approach to highly effective age assurance, strengthened safeguards for users and clearer guidance.

A5.42 Ofcom has issued guidance to help Part 3 services understand and meet their obligations under the Act.[359] We have taken a flexible, outcome-focused approach, allowing providers to choose the most appropriate methods based on their specific context, including their size, user base, and available resources.

A5.43 While our Part 3 HEAA Guidance sets out a non-exhaustive list of the kinds of age assurance that are capable of being highly effective, services may use alternative approaches, provided they can demonstrate that these meet the requirements of the Act. We also recognise that the age assurance sector is evolving, and more cost-effective solutions are likely to emerge as technologies develop.

A5.44 We consider that our measures as proposed address the risks and concerns raised by stakeholders. As such, we are not making any changes to them at this time.

---

[356] A member of the Philippine Survivor Network response to the June 2025 Consultation, p.22.
[357] Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.17.
[358] ACT – The App Association response to the June 2025 Consultation, p.9; BILETA response to the June 2025 Consultation, p.33; [✂]; [✂]; Name Withheld 9 response to the June 2025 Consultation, p.10; Name Withheld 26 response to the June 2025 Consultation, p.9; Online Dating and Discovery Association (ODDA) response to the June 2025 Consultation, p.8; [✂].
[359] Ofcom (2025), Guidance on highly effective age assurance.

A6. Increasing the effectiveness of safety defaults and supportive messaging

Further stakeholder responses received on this chapter by theme

Safety defaults measure

A6.1 Several stakeholders broadly supported safety defaults but raised concerns that children can disable them, which may reduce effectiveness and place responsibility on the child. Recommendations included adding child-friendly resources before settings are turned off and engaging with children to design features that encourage retention.[360] Some stakeholders welcomed defaults as essential for safety and impact measurement.[361]

Our response

A6.2 As explained in the June 2025 Additional Safety Measures Consultation (June 2025 Consultation) we are not consulting on the original details of the measure and maintain our current position that enabling safety defaults to be turned off is effective and proportionate. Our research provides strong indications that both adults and children largely retain safety-by-default options, at least when first exposed to them in a simulated online environment.[362] Our approach balances safety with children's rights and will be kept under review.

A6.3 See the December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement) for a full description of the importance of safety defaults.[363]

How the measures are applied

A6.4 In response to the June 2025 Consultation, the National Police Chiefs' Council (NPCC) and a government stakeholder raised the point that safety defaults should be applied automatically. The NPCC suggested applying them to all users by default with changes allowed only after being determined to be an adult using highly effective age assurance.[364]

---

[360] Barnardo's response to the June 2025 Consultation, pp.19-20; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.15; Marie Collins Foundation response to the June 2025 Additional Safety Measures Consultation (June 2025 Consultation), p.12; Marie Collins Foundation Lived Experience response to the June 2025 Consultation, p.2.

[361] Children's Commissioner's Office (CCO) response to the June 2025 Consultation, p.15; UK Finance response to the June 2025 Consultation, p.15.

[362] Ofcom (2026), 'Protective defaults for social media platforms', Behavioural Insights Discussion Paper. A vast majority of adult and child participants had retained all their default settings by the end of the experiment. Studies of this kind can provide useful evidence on attitudes, broad behavioural patterns, and the relative impact of different interventions. But are limited in their ability to capture the wider social, contextual and emotional factors that often influence behaviour in real-world settings, such as peer influence, social norms, rewards, and personal stakes. Findings should therefore be interpreted with these limitations in mind and viewed as indicative of how users may respond, rather than as a direct measure of real-world behaviour. See the technical report for more detail on methodology and findings.

[363] Ofcom (2024), December 2024 Statement, Vol 2, chapter 8: U2U settings, functionalities and user support

[364] National Police Chiefs' Council (NPCC) response to the June 2025 Consultation, p.14.

A government stakeholder recommended applying safety defaults automatically to all child users so that services do not need to "identify which children should benefit from these protections". It stated the proposed approach may create ambiguity on implementation and risk leaving some children unprotected.[365]

Our response

A6.5 We consider these suggestions are consistent with each option for implementation that we are proposing. However, we disagree with the suggestions it would be more effective for our recommendation to employ only one of the options as the recommended method to implement the safety defaults and supportive information measures. We maintain our position that having options is proportionate as they are both effective and gives services flexibility to choose the methods which best fits their service.

Age appropriateness

A6.6 Stakeholders emphasised that age appropriateness is critical, warning that a one-size-fits-all approach could weaken protections and reduce effectiveness. Other suggestions included tailoring default settings for specific age groups for example, having stricter controls (such as fixing the setting for those up to the age of 16 and defaults for 16 to 18 year olds) and making terms and conditions more understandable for children. Others noted that different age groups experience varying impacts on rights, such as freedom of expression, and urged Ofcom to consider these differences when applying restrictions.[366]

Our response

A6.7 In the December 2024 Statement, we decided not to take an age-differentiated approach to the measures (ICU F1 and F2) and explained that this was proportionate due to the severity of the harm.

A6.8 We will consider whether any future legislative changes require updates to our current position and will consult before making any such changes as appropriate.

A6.9 We will always ensure the measures remain proportionate and effective to protect all children from the risk of grooming with any changes we make in the future.

Self-declaration of age

A6.10 Stakeholders agreed that self-declaration of age is ineffective for determining whether a user is an adult or a child. The Information Commission's Office (ICO) acknowledged Ofcom's concerns about the effectiveness of self-declaration of age and supported the value of the proposed two options as stronger alternatives. The Internet Watch Foundation (IWF) also supported removing the provision limiting ICU F1 and F2 to services with existing age assurance, stating these protections should apply to all in-scope services in line with Part 3 HEAA Guidance.[367]

---

[365] [✂].

[366] Internet Watch Foundation (IWF) response to the June 2025 Consultation, p.50, Marie Collins Foundation Lived Experience Group response to the June 2025 Consultation, p.2; National Society for the Prevention of Cruelty to Children (NSPCC) response to the June 2025 Consultation, p.50; Open Rights Group response to the June 2025 Consultation, p.41.

[367] Information Commission's Office (ICO) response to the June 2025 Consultation, p.29; Internet Watch Foundation (IWF) response to the June 2025 Consultation, p.51; VerifyMy response to the June 2025 Consultation, p.3.

Our response

A6.11 We welcome the respondents' support of our proposals to address the ineffectiveness of self-declaration.

Grooming and emerging technologies

A6.12 The Institution of Engineering and Technology (IET) highlighted grooming and harm risks in immersive environments, stressing that, without strong safeguards, technologies like virtual reality (VR) and the metaverse could enable abuse and exploitation. It urged Ofcom to prioritise regulation, clarify legal responsibilities, and provide better tools and information for parents and users. Evidence cited included frequent exposure of children to abusive behaviour in VR spaces and concerns that current age limits are poorly enforced.[368]

Our response

A6.13 We maintain that our measures will ensure protections for children across a range of services which are assessed to be high or medium risk of grooming. Emerging technologies such as VR present potential risks to children, and we expect the principles of the measures to apply equally in these environments. We will continue to consider how best to address these risks as part of future policy development.

Relevance to other harms

A6.14 Several stakeholders suggested broadening the scope of the measures beyond grooming to address other harms, such as human trafficking[369], criminal exploitation, terrorism[370], and fraud.[371] A government stakeholder emphasised that grooming risks are not limited to sexual exploitation and recommended including criminal and interpersonal abuse, as well as radicalisation, citing evidence of increasing terrorism-related risks among minors.[372] The National Crime Agency (NCA) noted that while expansion could strengthen protections, its impact may be limited if services rely on self-declaration or downplay risks.[373]

Our response

A6.15 In the December 2024 Statement, we explained that the safety measures were designed to tackle grooming for the purpose of sexual exploitation and abuse of children. We recognised that there are other harms areas such as criminal exploitation and terrorism that these measures may help to mitigate.[374]

A6.16 The Illegal Harms Register of Risks (Illegal Harms Register) outlines the full risk assessment of where and how illegal harms manifest online. The characteristics of services are relevant to a range of risks of harm. Our position is set out in the December 2024 Statement.[375]

---

[368] Institution of Engineering and Technology (IET) response to the June 2025 Consultation, p.2.
[369] National Crime Agency (NCA) response to the June 2025 Consultation, p.23.
[370] [✂].
[371] UK finance response to the June 2025 Consultation, p.16.
[372] [✂].
[373] National Crime Agency (NCA) response to the June 2025 Consultation, p.23.
[374] Ofcom (2024), December 2024 Statement, Vol. 2, chapter 8: U2U settings, functionalities and user support.
[375] Ofcom (2024), Illegal Harms Register of Risks (Illegal Harms Register), chapter 2A: Grooming.

Network expansion prompts

A6.17 Snap, Inc. noted that network expansion prompts are essential for connecting users and a core functionality.[376] [✂].[377] A provider submitted that network expansion prompts are an important way in which users find people they know, and that removing them would require users to search for contacts individually.[378] A member of the Marie Collins Foundation Lived Experience Group raised questions about practical implementation and highly effective age assurance interaction, and suggested deterrence messaging for adults attempting to connect with children.[379]

Our response

A6.18 As explained in the June 2025 Consultation, we are not consulting on the details of the original measures, and we maintain our approach to network expansion prompts is proportionate given the severity of the harm.[380]

A6.19 As explained in our December 2024 Statement, the safety defaults measure (ICU F1) may affect user experience, including children's ability to make new connections online. However, connections can still be made on a service without network expansion prompts. The measure reduces the likelihood of unwanted or harmful contact between perpetrators and children. Given the serious nature of these harms, we consider this a proportionate and necessary protective step.

A6.20 We consider our measures to be the most effective and proportionate way to reduce the risk of grooming. We may consider additional measures in the future.

Costs of the measures

A6.21 The Association for UK Interactive Entertainment (Ukie) raised concerns that cost estimates did not account for differences "between sectors and risk levels".[381]

A6.22 One stakeholder said that our cost estimates neglected costs such as staff training and auditing.[382]

Our response

A6.23 Our measures are segmented by risk and are not sector specific as we consider every online service sector could potentially carry the risk of harms of online grooming. The Illegal Harms Register outlines the full risk assessment of where and how illegal harms manifest online. The characteristics of services are relevant to a range of risks of harm. Our position is set out in the December 2024 Statement.[383]

A6.24 Staff costs for implementing and maintaining the measures were considered in the June 2025 Consultation, either within the cost estimates of in-house provision or as part of a qualitative assessment of proportionality alongside cost estimates of third party age checks.

---

[376] Snap, Inc. response to the June 2025 Consultation, p.17.
[377] [✂].
[378] [✂].
[379] Marie Collins Foundation Lived Experience Group response to the June 2025 Consultation, p.3.
[380] Ofcom (2025), June 2025 Consultation, chapter 19, Increasing effectiveness for U2U settings, functionalities and user support.
[381] The Association for UK Interactive Entertainment (Ukie) response to the June 2025 Consultation, p.38.
[382] [✂].
[383] Ofcom (2024), Illegal Harms Register of Risks, chapter 2A: Grooming.

Rights assessment

A6.25 A stakeholder stated that they were concerned that the proposals disproportionately impact users' freedom of expression and association, particularly older child users. The stakeholder suggested that Ofcom consider different safety defaults for different age groups to limit the impact on older child users.[384]

A6.26 [✂].[385] They noted that this would have a disproportionate impact on both adult and child users' rights to freedom of expression.

A6.27 One stakeholder was concerned that the impact of the measure on restricting adult's freedom of expression had been underestimated.[386]

A6.28 Some stakeholders were concerned that our assessment had not considered the risk of children's data being exploited or the proposals deterring services from using functionalities that protect data, such as end-to-end encryption.[387]

A6.29 One stakeholder expressed concern that the proposals relating to highly effective age assurance lacked clear safeguards and transparency on how sensitive data would be protected.[388]

A6.30 Stakeholders were concerned with the general risks that came with the adoption of highly effective age assurance in relation to privacy, data security, and user surveillance.[389] One provider questioned the proportionality of Option A, on the basis that implementing the safety default and supportive information measures through highly effective age assurance for all users not determined to be adults would raise data protection, accessibility and effectiveness concerns.[390]

Our response

A6.31 We acknowledge the concerns around the proposals potentially disproportionately impacting both adult and child users' rights to freedom of expression, particularly older child users. However, as set out in the December 2024 Statement, our evidence suggests that a significant risk of harm from grooming is present for children of all age ranges.[391] Therefore, we maintain that the impact on freedom of expression is proportionate to the risk of harm from grooming.

A6.32 In relation to the potential impact of the measures on adult users' freedom of expression, the overall impact is proportionate to address the severity of the risk of grooming against children. Where highly effective age assurance is being implemented, we are recommending safeguards to allow adult users to appeal any decisions that assess them to be a child. Where the measures are applied to all users, the measures will not disproportionately impact adults as the restrictive settings are not fixed and the supportive messaging impact is negligible.

---

[384] Open Rights Group response to the June 2025 Consultation, pp.38-39.
[385] [✂].
[386] British and Irish Law Education and Technology Association (BILETA) response to the June 2025 Consultation, p.36;
[387] British and Irish Law Education and Technology Association (BILETA) response to the June 2025 Consultation, p.35; Open Rights Group response the June 2025 Consultation, p.39.
[388] [✂].
[389] [✂]; Name withheld 11 response to the June 2025 Consultation, p.1.
[390] [✂].
[391] Ofcom (2024), December 2024 Statement, Vol.2, chapter 8: U2U settings, functionalities and user support.

A6.33 We acknowledge stakeholders' concerns with risks to privacy where highly effective age assurance is used. Providers who choose to implement highly effective age assurance must comply with relevant data protection legislation and have regard to users' rights to privacy.

A6.34 Alongside the January 2025 Statement, we published the Part 3 HEAA Guidance, which demonstrates to providers how to implement highly effective age assurance and have regard to protecting users' privacy. The Part 3 HEAA Guidance highlights that providers must have regard to the importance of protecting users from a breach of statutory provision or rule of law concerning privacy (including data protection). Service providers must comply with data protection legislation and should familiarise themselves with ICO guidance in considering how data protection legislation applies to their age assurance process.

A6.35 The Part 3 HEAA Guidance points to data protection principles of the UK GDPR, the ICO's Children's Code, and the Commissioner's Opinion on Age Assurance for the Children's Code, which will assist providers in implementing age assurance, while protecting privacy of users and child users particularly.

A6.36 We have proposed safeguards in our Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes), as discussed in chapter 5: Highly effective age assurance in the Illegal Content Codes, that will help providers ensure that data security and user privacy are maintained where highly effective age assurance is implemented.

Compliance and enforcement

A6.37 In its response to the June 2025 Consultation, Barnardo's raised concerns about clarity on how Ofcom will monitor and enforce compliance. It urged that enforcement be supported by a full set of safety features, including moderation and reporting tools. [✂].[392]

Our response

A6.38 Our enforcement approach will be proportionate, evidence-based, and guided by our published enforcement framework. Compliance will be assessed on a case-by-case basis, and enforcement will focus on addressing serious risks of harm rather than applying blanket measures.

A6.39 We do not consider our approach excessive or likely to disproportionately impact freedom of expression. We will continue to monitor and review the impact of our proposals to ensure they remain balanced.

Risk of circumvention

A6.40 In their June 2025 Consultation responses, some stakeholders raised concern that users may attempt to bypass highly effective age assurance through methods such as virtual private network (VPN) use. They highlighted risks that perpetrators could create child accounts to interact with children and that restricting children's access might push them toward riskier services and that documentation requirements for age assurance may cause a barrier for users.[393]

[392] Barnardo's response to the June 2025 Consultation, p.20, [✂].
[393] Name Withheld 4 response to the June 2025 Consultation, p.9; Name Withheld 11 response to the June 2025 Consultation, p.1; National Police Chiefs' Council (NPCC) response to the June 2025 Consultation, p.13; Marie Collins Foundation Lived Experience Group response to the June 2025 Consultation, p.2.

Our response

VPN usage

A6.41 We are confident that our measures will still make children materially safer online. Although perpetrators may try to circumvent the measures by using a VPN, children in the UK will still be protected through the measures.

A6.42 In July 2026 we published our Use of Age Assurance Report.[394] In this we found that circumvention of age assurance appears low, with a relatively small minority of children reporting that they circumvent highly effective age checks or use VPNs to access restricted content of features. However, some activity may not be captured due to reporting bias.

A6.43 Evidence on circumvention techniques is limited but indicates that robust configuration and monitoring of age assurance processes is important to mitigate known and emerging risks.[395] Our Part 3 HEAA guidance is clear that services must not direct or encourage users to circumvent age assurance, including through the use of VPNs.[396]

A6.44 We will continue to monitor VPN usage and develop our evidence base on circumvention and displacement, but it would be a matter for the government to decide whether to take steps to address VPN usage by children.

A6.45 Further discussion of circumvention risks, including the use of VPNs, is set out in chapter 5: Highly effective age assurance in the Illegal Content Codes. Additionally, we address risks around circumvention of highly effective age assurance in our Part 3 HEAA Guidance, which requires services to identify and mitigate circumvention methods that are easily accessible to children and where it is reasonable to assume that children may use them.

Perpetrators creating child accounts

A6.46 The measure reduces the incentive for a perpetrator to create a child account for the purpose of interacting with other children. Where a perpetrator attempts to bypass the measure through registering as a child user, the relevant safety protections will be applied to their account by default. These protections create friction in interacting with other child users; for example, the account will not appear in network expansion prompts or connection lists.

A6.47 Even if a perpetrator turns the default settings off for their own account, the majority of children are likely to retain those default safety settings.[397] Consequently, a greater proportion of children are likely to be excluded from, or not exposed to, prompts encouraging network expansion. This will reduce the number of children available for perpetrators to identify and connect with through these features.

A6.48 Additionally, our approach reduces the risk of harmful activity moving to other services. This is because the risk assessment process identifies which services pose the greatest

---

[394] Ofcom (2026), Use of Age Assurance, p.48; Ofcom (2026), Children's use of VPNs.
[395] Ofcom (2026), Use of Age Assurance, p.61.
[396] Ofcom (2025), Guidance on highly effective age assurance, p16.
[397] Ofcom (2024), 'Behavioural insights to empower social media users. Testing tools to help users control what they see', Behavioural Insights Discussion Paper. Studies of this kind can provide useful evidence on attitudes, broad behavioural patterns, and the relative impact of different interventions. But are limited in their ability to capture the wider social, contextual and emotional factors that often influence behaviour in real-world settings, such as peer influence, social norms, rewards, and personal stakes. Findings should therefore be interpreted with these limitations in mind and viewed as indicative of how users may respond, rather than as a direct measure of real-world behaviour.

risks, ensuring that all high risk and larger medium risk services are still covered by the measure.

Documentation requirements

A6.49 Age assurance methods may require users to provide documentation which may create some friction for users. However, the age assurance methods employed on a service is the provider's decision and they will be best placed to determine which process is best suited for their users and service(s).

A6.50 Overall, having considered these responses our assessment on the robustness of highly effective age assurance remains unchanged, as the noted concerns do not significantly impact the effectiveness of our proposals and have been addressed in our Part 3 HEAA Guidance and the December 2024 Statement.[398]

How highly effective age assurance is applied

A6.51 In its June 2025 Consultation response, the Marie Collins Foundation recommended applying highly effective age assurance more broadly across services, suggesting that interventions should primarily target adult users rather than children and use of highly effective age assurance data to trigger protective actions throughout the user journey. It also noted that services already leverage user data for business purposes and should similarly use it to strengthen child protection.[399]

Our response

A6.52 We acknowledge the stakeholder's position on expanding highly effective age assurance. We maintain our current position on the recommended use of highly effective age assurance to implement the measures as an option for providers.

A6.53 We will continue to review its application to ensure any future recommendations remain proportionate and evidence based.

Effectiveness of highly effective age assurance

A6.54 Some stakeholders raised concerns about the effectiveness of highly effective age assurance. Name Withheld 9 noted that stored account activity cannot distinguish between children and adults and disputed that Option A would improve effectiveness.[400] Ukie argued that Option A could create unnecessary friction and intrusive data processing for all users, suggesting applying the measure to all may be simpler and safer, and emphasised that user education and parental tools have proven more effective than age verification in promoting safe play in the gaming industry.[401] However, Name Withheld 9 stated that neither option would increase the effectiveness of the measure.

Our response

A6.55 In our Part 3 HEAA Guidance we set out four criteria that services need to meet for their age assurance process to be considered highly effective: technical accuracy, robustness, reliability, and fairness.[402] These criteria establish a clear minimum standard for

[398] Ofcom (2025), Guidance on highly effective age assurance, p.20-21.
[399] Marie Collins Foundation response to the June 2025 Consultation, p.12.
[400] Name Withheld 9 response to the June 2025 Consultation, p.11.
[401] The Association for UK Interactive Entertainement (Ukie) response to the June 2025 Consultation, p.37.
[402] Ofcom (2025), Guidance on highly effective age assurance, p.10-11.

effectiveness. Service providers should ensure that the age assurance process as a whole fulfils each of the criteria, regardless of the method or combination of methods used.

A6.56 Furthermore, the Part 3 HEAA Guidance and January 2025 Age Assurance and Children's Access Statement (January 2025 Statement) outline that all age assurance methods which involve the processing of personal data and services should follow a data protection by design approach. This will assist service providers to implement highly effective age assurance while protecting user privacy in line with the data protection regime.

A6.57 On this basis, we maintain our position to recommend Option A as it offers a targeted application where highly effective age assurance can be deployed effectively.

Our approach to increasing the effectiveness of the measures

A6.58 In their responses, several stakeholders agreed with our approach to implementing the measures, stating it would strengthen child protections while giving providers flexibility to choose the most suitable method.[403]

A6.59 On the other hand, some stakeholders disagreed with our approach.[404] Some cited concerns about overreach, blanket restrictions, and lack of real choice.[405] Some argued that the evidence base for the proposals is weak and lacks independent scrutiny.[406] Barnardo's raised the risk of backlash if safety defaults apply to all users, urging Ofcom to work with providers to promote highly effective age assurance and reduce negative perceptions.[407]

Our response

A6.60 We have proposed two ways of implementing the measure and consider this to be a proportionate approach due to the reasons outlined in chapter 6: Increasing the effectiveness of safety defaults and supportive messaging. Given the severe impact grooming has and the important role these amendments will have in combatting grooming, we have decided that implementing this amendment will lead to significant benefits to users.

Tailoring the measures for children

A6.61 The Marie Collins Foundation and the National Society for the Prevention of Cruelty to Children (NSPCC) raised concerns that Option B (apply the two measures to all users) could make supportive information less tailored to children.

---

[403] A member of the Philippine Survivor Network response to the June 2025 Consultation, p.22; Barnardo's response to the June 2025 Consultation, p.16; The Children's Commissioner's Office (CCO) response to the June 2025 Consultation, p.23; Department of Justice Northern Ireland response to the June 2025 Consultation, p.15; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.15; Evangelical Alliance response to the June 2025 Consultation, p.10; ICO response to the June 2025 Consultation, p.29; International Justice Mission response to the June 2025 Consultation, p.4; Internet Matters response to the June 2025 Consultation, p.18; [✂], National Center for Missing & Exploited Children (NCMEC) response to the June 2025 Consultation, p.8; [✂]; National Police Chiefs' Council (NPCC) response to the June 2025 Consultation, p.15; Online Safety Network response to the June 2025 Consultation, p.24; [✂].

[404] Luethje, Y. response to the June 2025 Consultation, p.8; [✂].

[405] [✂]

[406] [✂]

[407] Barnardo's response to the June 2025 Consultation, p.20.

A6.62 Further to this, the NSPCC stated that while it recommends Option A (using highly effective age assurance), providers implementing Option B (applying measures to all users) should ensure any supportive information provided is accessible to children.[408]

Our response

A6.63 In the Illegal Content Codes, we recommend that supportive information be prominently displayed and easy for a child to understand (ICU F2.6). Therefore, in circumstances where information is produced for all users, providers must ensure it is understandable for child users.

A6.64 The measures ensure the supportive information is presented in a way that children can understand. Therefore, we have decided to keep the proposal as set out in the June 2025 Consultation. No further evidence or reasoning was provided with this feedback, and the measure remains unchanged.

[408] Marie Collins Foundation response to the June 2025 Consultation, p.11; NSPCC response to the June 2025 Consultation, p.41.

A7. Broadening content appeals

Further stakeholder responses received on this chapter by theme

Feedback on the definition of "illegal content proxy"

A7.1 In their responses to the June 2025 Additional Safety Measures Consultation (June 2025 Consultation), an industry stakeholder, an individual, and an industry trade association identified that they considered the definition of "illegal content proxy" to be overly broad or, as argued by Name Withheld 9 open to interpretation.[409]

A7.2 In its response to the June 2025 Consultation, the Association for UK Interactive Entertainment (Ukie) also argued that proxies need a clearer definition to avoid overextension, in essence suggesting that there is a difficulty in identifying illegal content proxies.[410]

Our response

A7.3 In the first instance, we note that we have already published documents where we have provided definitions for "proxy content", most notably in our Illegal Content and Protection of Children Codes of Practice for user-to-user services (collectively referred to as the Codes) and in the introduction to the chapter of our June 2025 Consultation. We have reiterated this in paragraphs 7.2-7.3 in chapter 7: Broadening content appeals.

A7.4 We consider that this definition gives providers flexibility to assess whether content is in breach of their terms of service, rather than to assess whether it is illegal or harmful to children as defined by the Online Safety Act 2023 (the Act). We recognise that many service providers design their terms of service and guidelines both to comply with existing laws in multiple jurisdictions and to meet their own commercial needs. As such, the definition of "proxy content" is intentionally broad and open to interpretation to grant providers this flexibility. We do not consider it would be possible to narrow this definition without removing this flexibility.

A7.5 In response to Ukie, we do not consider that being more prescriptive in our definition of illegal content proxy would address provider difficulties in identifying such content. Narrowing the definition would reduce the flexibility that the definition is intended to provide.

A7.6 It is up to providers to decide whether to make decisions based on proxies. This requires their terms of service to be cast broadly enough to necessarily cover illegal content and content harmful to children. Providers have a duty to enforce their terms of service, and therefore providers deciding to make decisions based on proxies have a duty to act based on proxy content that they determine breaches their terms of service. We do not consider that changing the definition of "proxy content" will have an impact on (or remove) these duties or have an impact on the difficulty referred to by Ukie.

---

[409] Association for UK Interactive Entertainment (Ukie) response to the June 2025 Consultation, pp.39-41; Name Withheld 9 response to the June 2025 Additional Safety Measures Consultation, pp.13-14; Google LLC response to the June 2025 Consultation, pp.36-37.

[410] Ukie response to the June 2025 Consultation, pp.39-41.

A7.7 We maintain that making the amendments as proposed is the correct approach, and do not consider that changing or narrowing the definitions for "proxy content" would benefit users or providers.

Comments on amendment effectiveness

A7.8 In its response to the June 2025 Consultation Ukie raised concerns about how the proposals could increase the burden on providers, especially gaming services. It suggested that the proposals, on top of existing systems and processes, could require providers to offer appeals for minor or clear enforcement decisions.[411]

Our response

A7.9 While we recognise the amendments could increase the administrative burden on service providers, a robust content appeals function is nevertheless necessary to comply with the Act. As explained in our June 2025 Consultation, this might incur costs. For more detail, see the section titled 'Impacts and costs' in chapter 7: Broadening content appeals.

A7.10 To clarify, the amendments only apply where content has been moderated due to a determination by the service that it is illegal content proxy or content harmful to children proxy. This approach does not recommend content appeals for additional content (that would not be considered a proxy), that may be moderated for violating a provider's wider terms of service.

A7.11 Ukie's response also called for the amended measures to be limited to situations where there is genuine uncertainty or discretion in the moderation decisions.[412] However, it is not clear to us how service providers would apply this standard in practice.

A7.12 Under the Act, a provider has a duty to operate a complaints procedure that allows for users who have generated, uploaded or shared content, to complain if that content is taken down on the basis that it is illegal content[413] or content harmful to children.[414] These duties do not distinguish between "certain" moderation decisions and "uncertain" ones. As such, it would be inconsistent with those duties to draw that distinction when it comes to proxy content.

A7.13 We acknowledge that service providers have existing systems and processes to handle content appeals and highlight that they will not need to set up additional systems and processes as a result of the amendments.

A7.14 We therefore maintain that making the amendments will deliver significant benefits to users while maintaining flexibility for providers.

Supporting assessed impacts of proposals

A7.15 In their responses, an individual, an industry stakeholder, and a civil society organisation stated their support for our assessment of the likely impacts of these amendments. Digital Resilience in Education, [✂] and [✂] agreed with the assessment of impacts, with Digital Resilience in Education going on to suggest that a content appeals function may improve trust in the service and generally improve the service through feedback.[415]

---

[411] Ukie response to the June 2025 Consultation, pp.39-41.
[412] Ukie response to the June 2025 Consultation, pp.39-41.
[413] Section 21(4)(c) of the Act.
[414] Section 21(5)(c) of the Act.
[415] Digital Resilience in Education response to the June 2025 Consultation, pp.17-18; [✂]; [✂].

Our response

A7.16 We welcome this support of our assessment of the likely impacts of the amendments.

Disagreement with assessed impacts of proposals

A7.17 Two individual respondents disagreed with our assessment of the likely impacts and costs of the amendments, with [✂] saying that [✂],[416] and [✂].[417] Neither stakeholder provided evidence for their disagreement. Two respondents – an individual and a trade association – also made comments relating to the demands on content moderation teams as a result of increased content appeals.[418] An individual stakeholder raised concerns about [✂].[419]

Our response

A7.18 In our June 2025 Consultation, we said that service providers cannot comply with their duties under the Act without a robust content appeals function. We explained they would therefore incur the costs of implementing existing content appeals measures largely as a result of requirements of the Act. This means that any such costs incurred would not be a result of choices over which we have regulatory discretion.

A7.19 Where disagreement with the assessment of amendment impacts was based on more specific reasoning, we have addressed this in chapter 7: Broadening content appeals. However, we cannot give a meaningful response to disagreement with our assessment of the amendments' impacts that does not offer supportive evidence or further context.

A7.20 As set out in paragraph 7.42 of chapter 7: Broadening content appeals, we also expect the majority of service providers of all sizes will be able to use their existing systems and processes to deal with additional content appeals arising as a result of the amendment. The type of content appeals system that is appropriate is likely to vary between services according to size, risk level, and other factors.

A7.21 While the number of content appeals received could increase as a result of this amendment to ensure timely appeals for both harmful/illegal content as well as proxies (with associated costs to services in terms of content moderation resourcing) these costs can be considered to be arising from a direct requirement of the Act. Our assessment of costs therefore remains unchanged.

A7.22 Finally, we do not consider that the amendments constitute an undue interference with freedom of expression. They act as a safeguard against disproportionate interference with freedom of expression that could arise from other measures if they are implemented without these amendments. For detail on these measures, please see Table 7.2: Amendments for measures ICU D8.4 and D10.2 and PCU D8.4 and D10.2 to include proxy content in chapter 7: Broadening content appeals.

---

[416] [✂].
[417] [✂].
[418] Are, C. (Dr) response to the June 2025 Consultation, pp.26-28; UK Finance response to the June 2025 Consultation, p.17.
[419] [✂].

General disagreement with proposals

A7.23 Two individual stakeholders in their responses stated their disagreement with the proposals. Luethje, Y. disagreed with the amendments, but with no explanation or evidence, and [✂] more generally [✂].[420]

Our response

A7.24 Where disagreement with the proposals was based on more specific reasoning, we have addressed this in chapter 7: Broadening content appeals. We cannot give a meaningful response to disagreement that does not offer explanation or further context.

A7.25 We have sought to more directly respond to the issues identified in [✂]'s response in the sections of the chapter that correlate to the issues they have identified, most notably in section titled 'Our reasoning' in chapter 7: Broadening content appeals.

A7.26 Overall, we do not consider that changing the amended measures would address the issues raised by [✂] without losing significant benefits to users.

Transparency of the amended measures

A7.27 In their responses, an individual and an advocacy group made comments relating to transparency of content appeals. [✂], as well as arguing that [✂].[421] The Open Rights Group also said content appeals should be considered within a time limit and subject to independent adjudication. Further, it suggested services should publish the number of content appeals they receive and uphold in their transparency reporting.[422]

Our response

A7.28 We expect that our amendments will help to ensure a level of transparency because of the measures that ensure content appeals are carried out in an appropriate, timely, and transparent manner. See chapter 7: Broadening content appeals for details on these measures (ICU D8, PCU D8, ICU D9, PCU D9, ICU D10, PCU D10, ICU D12, and PCU D13).

A7.29 Regarding comments from the Open Rights Group, we do not consider it would be proportionate to prescribe independent adjudication of content appeals, given the immense resource requirement this would place both on adjudicators and on service providers.

A7.30 Ofcom will consider the exercise of its transparency powers in due course.

Penalising malicious use of content appeals

A7.31 In its response, UK Finance suggested that strikes against users of unsuccessful content appeals should be used to discourage overuse of content appeals.[423]

Our response

A7.32 We recognise that expanding users' ability to make content appeals may result in an increase in the number of content appeals made by users, which may increase the work of providers' moderation teams. However, we do not consider it would be fair or consistent

[420] [✂]; Luethje, Y. response to the June 2025 Consultation, p.9.
[421] [✂].
[422] Open Rights Group response to the June 2025 Consultation, p.46.
[423] UK Finance response to the June 2025 Consultation, p.17.

with the Act for providers to penalise users for making content appeals that are not upheld.

Harm-specific considerations

A7.33 In its response relating to harm-specific content appeals, South West Grid for Learning (SWGfL) suggested that content appeals for non-consensual intimate imagery (NCII) should be time-bound and recommended that services retain match artefacts, such as hash IDs or decision notes, for enforcement purposes.[424]

Our response

A7.34 We would direct SWGfL to Section D of each of our Codes,[425] where we have made Code recommendations on determining appeals, and on quality assurance of hash-matching for intimate image abuse (IIA) in our Statement: Detecting intimate image abuse.[426]

A7.35 Ofcom's role under the Act is to regulate service providers' systems and processes, not their decisions about individual items of content, and we therefore do not consider it proportionate to make amendments per SWGfL's recommendation.

Accuracy of content appeals

A7.36 In its response, UK Finance suggested the need for systems to be put in place to ensure content appeal review accuracy and ensure content appeals are reviewed to ensure content is not fraudulent content.[427]

Our response

A7.37 While we recognise the capacity for harm posed by fraudulent content, we do not consider it proportionate to expect providers consider certain content appeals separately from others.

A7.38 Additionally, we consider that the measures outlined in paragraphs 7.27g-k in chapter 7: Broadening content appeals (ICU D8, PCU D8, ICU D9, PCU D9, ICU D10, PCU D10, ICU D12, and PCU D13) will ensure that content appeals are dealt with in an accurate and timely manner, regardless of the type of harm that led to the enforcement being appealed.

Other comments

A7.39 UK Finance said Ofcom encourages but does not require services to offer content appeals, as well as suggesting "illegal content" should mention all types of fraud.[428]

Our response

A7.40 Firstly, the Act requires service providers to offer content appeals to users.

A7.41 Our Illegal Harms Register of Risks[429] and our Illegal Content Judgements Guidance[430] describe all the types of fraud that give rise to priority illegal content.

---

[424] South West Grid for Learning (SWGfL) response to the June 2025 Consultation, p.22.
[425] Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes), Measures ICU D1-D14.9; Protection of Children Codes of Practice for user-to-user services (Protection of Children Codes), Measures PCU D1-D14.
[426] Ofcom (2026), May 2026 Statement, Detecting Intimate Image Abuse.
[427] UK Finance response to the June 2025 Consultation, p.17.
[428] UK Finance response to the June 2025 Consultation, p.17.
[429] Ofcom (2025), Illegal Harms Register of Risks, p.234-254.
[430] Ofcom (2025), Illegal Content Judgements Guidance, p.101-119.

A7.42 Overall, we do not consider these comments to be suggesting changes to our amendments, nor taking issue with them.

A8. Introduction to proactive technology

Further stakeholder responses received on this chapter by theme

Definition of proactive technology

A8.1 One industry stakeholder and one public body expressed concerns about the definition of proactive technology.[431] In addition, one civil society stakeholder asked for clarification regarding the difference between proactive technology and Artificial Intelligence (AI).[432]

Our response

A8.2 The definition of proactive technology is set out clearly in the Online Safety Act 2023 (the Act).[433] Our measures are designed around this definition. As noted in chapter 8: Introduction to proactive technology of the statement, broadly speaking proactive technology refers to content identification technology, user profiling technology, or behaviour identification technology. These are all defined terms in the Act and we do not consider that the definitions are limited to hash matching and AI detection. While the use of AI is broader than just for proactive technology, we recognise AI is used for content moderation purposes including detecting content.[434]

A8.3 Regarding Image Angel's recommendation that the definition of proactive technology is broadened to include traceability and deterrence technologies, there are no limitations in the Act and we will consider and/or recommend all technologies that match our intended measures and outcomes, so long as they are proportionate. We are actively researching these technologies already and published a discussion paper which included research into watermarking technology in July 2025.[435] We may recommend such measures in the future if needed.

End-to-end encryption

A8.4 Several stakeholders suggested the proactive technology measures should apply to end-to-end encrypted services, and some considered technology is available for this.[436]

---

[431] Image Angel response to the June 2025 Consultation on Additional Safety Measures, pp. 6-7.; [✂].

[432] Marie Collins Foundation Lived Experience Group response to the June 2025 Consultation on Additional Safety Measures, p. 5.

[433] Section 231 of the Act.

[434] Cambridge Consultants, 2019. Use of AI in online content moderation: 2019 report produced on behalf of Ofcom.

[435] Ofcom, 2025. Deepfake Defences 2: The Attribution Toolkit.

[436] British and Irish Law Education and Technology Association (BILETA) response to the June 2025 Additional Safety Measures Consultation, pp. 36, 38-39; Department of Justice for Northern Ireland response to the June 2025 Additional Safety Measures Consultation, pp. 7-8; International Justice Mission response to the June 2025 Additional Safety Measures Consultation, pp. 7, 13-15; Internet Watch Foundation response to the June 2025 Additional Safety Measures Consultation, pp. 5, 15-16; Marie Collins Foundation Lived Experience Group response to the June 2025 Consultation, p. 5; Marie Collins Foundation response to the June 2025 Additional Safety Measures Consultation, p. 8; [✂]; Scottish Government response to the June 2025 Additional Safety

Conversely, we received feedback from other stakeholders who disagreed with the use of proactive technology on end-to-end encrypted services.[437] Further, several stakeholders raised end-to-end encryption as a specific example of where service providers might cite technical infeasibility.[438]

Our response

A8.5 We recognise that there is mixed feedback on how measures should apply in these environments but note that all in-scope service providers need to adhere to the duties in the Act.

A8.6 As stated in chapter 8: Introduction to proactive technology in the section titled 'Analytical framework for making recommendations regarding the use of proactive technology', our recommendations only apply where it is technically feasible for a provider to implement them. Several measures we are recommending as part of this statement relate to the use of proactive technology. These measures do not apply to providers where it is not technically feasible to analyse user-generated content present or disseminated on the service to assess if that is content of a particular kind. This is particularly the case where such changes would materially compromise the security of that service. When considering measures, we also consider wider laws on the access and storage of information on terminal equipment such as mobile devices.[439]

A8.7 We do not consider that it would be technically infeasible to implement a measure because doing so may require a change in the design and/or operation of a service. Where a service provider claims that it is technically infeasible for it to implement proactive technology, we have the power to investigate this. Should we then find that it is technically feasible for the provider to implement proactive technology, the measure will apply to them.

A8.8 In addition, Ofcom can only recommend the use of proactive technology for publicly communicated content. While end-to-end encryption is not necessarily private in all instances, these measures will not apply when it is used for private communications.[440] We explain this in more detail in chapter 8: Introduction to proactive technology in the section titled 'Analytical framework for making recommendations regarding the use of proactive technology'.

Scanning of private communications

A8.9 Multiple civil society stakeholders, one industry stakeholder and one law enforcement stakeholder acknowledged that Ofcom could not recommend scanning of private

---

Measures Consultation, p. 4; UK Finance response to the June 2025 Additional Safety Measures Consultation, p. 2; We are Survivors response to the June 2025 Additional Safety Measures Consultation, p. 3.

[437] ACT response to the June 2025 Additional Safety Measures Consultation, pp. 3-4; European Digital Rights Organisation response to the June 2025 Consultation, pp. 1-2; Google LLC response to the June 2025 Consultation, pp. 5-6, 16-17; [✂]; [✂]; Open Rights Group response to the June 2025 Consultation, p. 15; [✂]; Thompson, A. response to the June 2025 Additional Safety Measures Consultation, p. 3.

[438] ACT response to the June 2025 Consultation, pp. 3-4; European Digital Rights Organisation response to the June 2025 Consultation, p. 1; Google LLC response to the June 2025 Consultation, p. 5, 8; Internet Watch Foundation response to the June 2025 Consultation, p. 16; [✂]; National Society for the Prevention of Cruelty to Children (NSPCC) response to the June 2025 Additional Safety Measures Consultation, pp. 32-33.

[439] Privacy and Electronic Communications (EC Directive) Regulations, 2003.

[440] For an explanation of our approach to content communicated privately, see the section entitled 'Content communicated privately'.

communications, but strongly encouraged it due to the risk of abuse in these environments.[441] A member of the Philippine Survivor Network suggested smaller chat apps or forums where content can spread privately should be included, while the NSPCC explained that perpetrators often move children from public spaces to less moderated private ones (like gaming services) to build relationships and obtain personal details.[442]

A8.10 Two civil society stakeholders and one industry stakeholder argued that private communications should not be scanned by proactive technology, referencing that the Act distinguishes between public and private communications.[443] Open Rights Group and European Digital Rights Organisation also questioned why Ofcom had outlined in the June 2025 Consultation that providers could choose to extend proactive technology to private communications.[444] Google LLC stated that proactive technology should be balanced with protecting users' privacy and freedom of expression.[445]

A8.11 One industry stakeholder requested clarification on whether providers would be required to use proactive technology on private communications.[446]

Our response

A8.12 The Act is clear that Ofcom is only able to recommend the use of proactive technology for communications sent publicly.[447] Schedule 4 to the Act, paragraph 13 sets out the constraints on our power to recommend measures that describe the use of proactive technology as a way (or one of the ways) of complying with a relevant duty. These include that the measure may not recommend the use of technology to analyse user-generated content communicated privately, or metadata relating to such content.

A8.13 Regarding feedback on the need to include smaller chat apps or forums where content can spread privately, we recognise that the severity and reach of harm to users on these services remains significant. However, we consider the resource requirements needed to implement proactive technology on these services are likely to be significant and may not be proportionate. However, we consider that applying the measures to large, medium risk services will still deliver significant benefits to UK users, including a material reduction in the relevant harm. While our proactive technology measures do not currently apply to

---

[441] A member of the Philippine Survivor Network response to the June 2025 Additional Safety Measures Consultation, p. 13; [✂]; Barnardo's response to the June 2025 Additional Safety Measures Consultation, p. 7; European Digital Rights Organisation response to the June 2025 Consultation, p. 1; Google LLC response to the June 2025 Consultation, pp. 4-5, 14; Image Angel response to the June 2025 Consultation, p.8; International Justice Mission response to the June 2025 Consultation, p. 10; [✂]; NSPCC response to the June 2025 Consultation, p. 22; Open Rights Group response to the June 2025 Consultation, pp. 19-20; [✂].

[442] A member of the Philippine Survivor Network response to the June 2025 Consultation, p. 13; [✂]; NSPCC response to the June 2025 Consultation, pp. 20-21.

[443] European Digital Rights Organisation response to the June 2025 Consultation, p. 1; Google LLC response to the June 2025 Consultation, pp. 4-5,14; Open Rights Group response to the June 2025 Consultation on, pp. 19-20.

[444] European Digital Rights Organisation response to the June 2025 Consultation, p. 1; Open Rights Group response to the June 2025 Consultation, pp.20-21.

[445] Google LLC response to the June 2025 Consultation, pp. 4-5, 14.

[446] Snap Inc. response to the June 2025 Consultation, p. 5.

[447] Schedule 4 to the Act, paragraph 13(4). We have set out guidance which is intended to assist services in deciding whether content is communicated 'publicly' or 'privately' for this purpose: Guidance on content communicated 'publicly' and 'privately' under the Online Safety Act.

these services, we have the ability to revisit this in future iterations of the Codes of Practice.

A8.14 We provide an explanation of the constraints on Ofcom's powers regarding proactive technology, including the scanning of private communications, in chapter 8: Introduction to proactive technology in the section entitled 'Analytical framework for making recommendations regarding the use of proactive technology'. Further information on how Ofcom interprets content communicated publicly and privately is set out in our published guidance.[448]

'Pre-screening' content

A8.15 We received responses from some stakeholders about 'pre-screening' content. The Marie Collins Foundation argued that proactive technology should be used to "pre-screen" content, noting for livestreams proactive technology could build in short transmission delays to allow screening to take place before content is streamed.[449]

A8.16 GitHub cautioned against the scanning of content pre-upload.[450]

Our response

A8.17 We are not prescriptive about whether providers should pre-moderate content on their service. However, we do recommend that providers should ensure that content and/or relevant inputs that are generated on, uploaded to or shared on the service (or that a user seeks to generate, upload or share) after the proactive technology is implemented are analysed before or as soon as practicable after, relevant content can be encountered by United Kingdom users of the service."[451]

Scanning of content at device level

A8.18 One independent body, one civil society stakeholder and one academic stakeholder argued content should be scanned at a device level.[452] They emphasised the need to detect or disrupt harmful content at an earlier stage before it is published. The Commissioner Designate for Victims of Crime Northern Ireland added that this would be more effective than removing content after publication, while BILETA and the International Justice Mission argued it could offer protection without causing excessive surveillance.[453]

A8.19 One individual recommended we clarify in our Draft Proactive Technology Guidance that client-side scanning is out of scope unless new primary legislation approves it.[454]

---

[448] We have set out guidance which is intended to assist services in deciding whether content is communicated 'publicly' or 'privately' for this purpose: Guidance on content communicated 'publicly' and 'privately' under the Online Safety Act.

[449] Marie Collins Foundation response to the June 2025 Consultation, p. 7.

[450] GitHub's response to the June 2025 Additional Safety Measures Consultation, p. 2.

[451] See the Illegal Content Code of Practice for user-to-user services: Proactive Technology (unknown content), Measure: ICU PT1

[452] BILETA response to the June 2025 Consultation, pp. 6-7; International Justice Mission response to the June 2025 Consultation, pp. 15-16; The Commissioner Designate for Victims of Crime Northern Ireland response to the June 2025 Consultation, p. 5.

[453] BILETA response to the June 2025 Consultation, pp. 6-7; International Justice Mission response to the June 2025 Consultation, pp. 15-16; The Commissioner Designate for Victims of Crime Northern Ireland response to the June 2025 Additional Safety Measures Consultation, p. 5.

[454] Edwards, L. response to the June 2025 Additional Safety Measures Consultation, p. 3.

Our response

A8.20 While we recognise the evidence presented by stakeholders on the importance of detecting harmful content at the earliest stage, Ofcom does not have powers under the Act to regulate devices. Ofcom will keep its measures under review in light of any future legislative changes that may require updates to our current position, and will consult before making any such changes as appropriate.

Transparency around proactive technology use

A8.21 Several stakeholders (including those from civil society, individuals, and academia) argued that there should be transparency about the use of proactive technology deployed under the proactive technology measures.[455] They recommended that we require providers to be transparent to users about a variety of details about the proactive technology used on the service, including how technology is trained and evaluated; precision and recall rates; bias audits; error, takedown and appeals rates; general public performance benchmarking; and false positive and false negatives rates.[456]

Our response

A8.22 As outlined in our December 2024 Statement on Protecting People from Illegal Harms (December 2024 Statement) and our April 2025 Statement on Protecting Children from Harms Online (April 2025 Statement), providers have a duty in the Act to include provisions in their terms of service about the proactive technology they use to comply with their illegal harms and children's safety duties.[457] We consider that this provides an appropriate level of transparency to users about how proactive technology is being used on a service, including proactive technology a provider deploys in accordance with our measures.

A8.23 Some stakeholders asked for more specific details about the proactive technology deployed in accordance with our measures to be published to users. We consider that excessive levels of detail in terms of service about how systems and processes operate or are being used to protect users may require a disproportionate use of resources to keep up to date. This is particularly relevant where safety technology and processes are constantly evolving. We also recognise that too much detail about how proactive technology is deployed in terms of service may allow perpetrators to use the information to circumvent these safety measures. We have therefore decided not to recommend that providers publish specific details to users about how proactive technology is used on their service beyond that which they are required to publish in their terms of service to meet their duties in the Act.

---

[455] BILETA response to the June 2025 Consultation, p. 8; Edwards, L. response to the June 2025 Consultation, p. 3; Glitch response to the June 2025 Additional Safety Measures Consultation, pp. 4-7, 11-12; Online Responsibility Network response to the June 2025 Additional Safety Measures Consultation, p. 3; Refuge response to the June 2025 Additional Safety Measures Consultation, p. 7; Respondents to the Open Rights Group Campaign response to the June 2025 Consultation, p. 2; UK Finance response to the June 2025 Consultation, p. 2,7.

[456] BILETA response to the June 2025 Consultation, p. 8; Edwards, L. response to the June 2025 Consultation, p. 3; Glitch response to the June 2025 Consultation, pp. 4-7, 11-12; Online Responsibility Network response to the June 2025 Consultation, p. 3; Refuge response to the June 2025 Consultation, p. 7; Respondents to the Open Rights Group Campaign response to the June 2025 Consultation, p. 2; UK Finance response to the June 2025 Consultation, p. 2, 7.

[457] Sections 10(7) and 12(12) of the Act.

Relationship between our proactive technology measure to detect image-based CSAM content and our hash matching measures

A8.24 One industry stakeholder called for clarity on the relationship between the hash-matching measures and the proactive technology measures.[458]

Our response

A8.25 As part of our Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes), we recommend the use of perceptual hash matching to analyse relevant content to assess whether it is CSAM and swiftly take down detected content that is CSAM.[459] Hash matching facilitates the detection of known image-based CSAM only. We are therefore recommending the measure on deploying proactive technology to detect unknown image-based CSAM. We acknowledge that proactive technology that is designed and deployed to detect unknown CSAM is also capable of detecting known CSAM. However, to ensure the detection and removal of CSAM is as quick and effective as possible, we consider it is proportionate that in-scope services continue to use our recommended hash matching for known CSAM measure (ICU C9) alongside proactive technology for unknown image-based CSAM. Hash matching is a well-established industry practice that is highly accurate at detecting known CSAM and enables automated removal and reporting of that content without further layers of moderation or human review. Hash matching is also necessary to protect child users who may appear to be older than they are, as review of the content may not be sufficient on its own to identify it as CSAM. Proactive technology is vital for the detection of unknown CSAM but should be implemented alongside hash matching as it may not always detect known content with the same level of accuracy or confidence as hash matching.

A8.26 We consider that, taken together, these measures complement one another. Any content detected by proactive technology in line with our proactive technology measure for detecting image-based CSAM and subsequently determined to be CSAM by a service's content moderation function should be reported to the National Crime Agency (NCA) or a foreign agency with corresponding functions. Further, service providers can include hashes created from this content for inclusion in a database to prevent its further circulation, in accordance with our measure on using hash matching to detect and remove CSAM.

[458] Middle Tech Coalition response to the June 2025 Additional Safety Measures Consultation, p. 5.

[459] See the Illegal Content Codes Measure ICU C9: perceptual hash matching measure for CSAM.

A9. Deployment of proactive technology to detect image-based CSAM

Further stakeholder responses received on this chapter by theme

Inclusion of additional harms in the measure

A9.1 Several stakeholders proposed that additional priority illegal harms should be included in scope of the measures.[460]

A9.2 Several stakeholders proposed that additional harms to children should be included in scope of the measures.[461]

A9.3 Three stakeholders called on Ofcom to remain open to extending measures to additional harms in the future:

- The Online Safety Network said Ofcom must commit to expanding its approach over time using evidence to keep up with new types of harm.[462]
- The Evangelical Alliance recommended ongoing review of new emerging harms such as online coercion, financial exploitation and self-harm where proactive technology could also apply.[463]
- [✂].[464]

[460] This included hate, [✂], [✂], slavery stalking, animal cruelty content, illegal self-harm content, harassment, intimate image abuse, and terrorist content. A member of the Philippine Survivor Network response to the June 2025 Consultation, p. 12; The Antisemitism Policy Trust response to the June 2025 Consultation, p. 3; BILETA response to the June 2025 Consultation, p. 9; Common Sense Media's response to the June 2025 Consultation, p. 5, 6; [✂]; Glitch response to the June 2025 Consultation, p. 10; [✂]; Image Angel response to the June 2025 Consultation, p. 7; Internet Watch Foundation response to the June 2025 Consultation, pp. 28-29; Molly Rose Foundation response to the June 2025 Consultation, pp. 8, 13-14; [✂]; NSPCC response to the June 2025 Consultation, pp. 26-28; Online Safety Network response to the June 2025 Consultation, p. 13; Refuge response to the June 2025 Consultation, pp. 5-7; Samaritans response to the June 2025 Additional Safety Measures Consultation, p. 4; Social Media Animal Cruelty Coalition response to the June 2025 Consultation, pp. 6-9; [✂]; The Commissioner Designate for Victims of Crime Northern Ireland response to the June 2025 Consultation, p. 5; [✂].

[461] This included all priority content harmful to children and non-designated content harmful to children. A member of the Philippine Survivor Network response to the June 2025 Consultation, p. 12; Internet Matters response to the June 2025 Consultation, p. 9; Molly Rose Foundation response to the June 2025 Consultation, pp. 1-2; 6-9, 13-15; NSPCC response to the June 2025 Consultation, p. 26-29; Samaritans response to the June 2025 Consultation, p. 4.

[462] Online Safety Network response to the June 2025 Additional Safety Measures Consultation, p. 13

[463] Evangelical Alliance response to the June 2025 Additional Safety Measures Consultation, p. 3

[464] [✂].

A9.4 Conversely, various stakeholders expressed concerns about the possibility that we may expand the scope of harms in the future, particularly to illegal hate offences.[465]

A9.5 The Molly Rose Foundation rejected Ofcom's justification that extending proactive technology to all 130 offences under the Online Safety Act (the Act) was disproportionate, arguing that this reasoning was flawed and counterproductive given the close link between suicide and self-harm content. It said it was concerned by Ofcom's justification that prioritising certain harms aligned with its eight targets for immediate action, arguing this conflicted with the inclusion of illegal suicide content in one of the targets and risked bypassing Parliament's intent to cover a wide range of offences under the Act.[466]

A9.6 The Molly Rose Foundation said Ofcom repeatedly chose not to adopt best practice safety measures already used by some providers, including their use of proactive technology beyond the limited scope of illegal harms and Primary Priority Content. It expressed concern that Ofcom's proposals could undermine the effectiveness of existing Codes, particularly by limiting the scope of proactive technology measures, which it said may reduce the effectiveness of current recommender systems and content moderation rules.[467]

A9.7 The Molly Rose Foundation strongly contested Ofcom's claim that effective, accurate and lacking in bias proactive technology was more likely to be available for currently prioritised harms, citing its own 2024 research showing that 71.4% of moderation decisions on suicide and self-harm content were at least partially automated. It argued this contradicted Ofcom's principles-based approach, which could have supported a broader application and ensured the regime is not unnecessarily 'frozen in time' until further harms are brought into scope in a future consultation.[468]

Our response

A9.8 We welcome comments from stakeholders about the inclusion of specific harms in scope of the measure. For the reasons we set out in chapter 9: Deployment of proactive technology to detect image-based CSAM, in the section entitled 'Our decision', we are only confirming the amended proactive technology measure for the purpose of detecting unknown image-based CSAM at this time. We are revising our proposals with respect to other harms and intend to address stakeholder feedback related to the inclusion of additional harms when we consult in Spring 2027.

AI-generated content

A9.9 Three stakeholders requested clarification that content generated by artificial intelligence (AI) would be captured by our proactive technology measures:

- The British and Irish Law Education and Technology Association (BILETA) said harms were defined in relation to identifiable users, but it argued that synthetic agents like AI

[465] BILETA response to the June 2025 Consultation, pp. 9-10; Francis, S. response to the June 2025 Consultation, p. 7; [✂]; Google LLC response to the June 2025 Consultation, pp. 13-14; [✂]; Klaushofer, A. response to the June 2025 Consultation, p. 4; Luethje, Y. response to the June 2025 Consultation, p. 3; Mack, S, Dr. response to the June 2025 Consultation, p. 3; [✂]; Name Withheld 26 response to the June 2025 Consultation, p. 5; Name Withheld 27 response to the June 2025 Consultation, pp. 4-5; Open Rights Group response to the June 2025 Consultation, pp. 14,17-18; Together Campaign Declaration response to the June 2025 Consultation, p. 2.

[466] Molly Rose Foundation response to the June 2025 Consultation, p. 8.

[467] Molly Rose Foundation response to the June 2025 Consultation, p. 6.

[468] Molly Rose Foundation response to the June 2025 Consultation, p. 8.

avatars could also cause similar harm to trust, dignity, and discourse. It urged Ofcom to confirm that its proactive technology duties apply to synthetic or AI-generated livestreams, so regulation keeps pace with evolving technologies.[469]

- Common Sense Media stated that deepfakes represent a gap in Ofcom's recommendation and specifically mentioned AI-generated CSAM. It cited the California CSAM AI Law which made it illegal to possess or distribute AI generated CSAM and stated that without it, offenders possessing AI generated CSAM of real children could avoid conviction.[470]
- NSPCC said Ofcom's previous Statement indicated some AI services and chatbots are classified as search rather than user-to-user under the Act, making it unclear whether children will be adequately protected from illegal harms such as grooming and suicide encouragement, and harmful content under current proposals. It recommended Ofcom provide greater clarity on which AI services fall under the scope of these measures and highlight any limitations caused by the legislation's scope.[471]

Our response

A9.10 Content generated using AI is in scope of the Act and should be captured by the proactive technology measure in the same way as human-generated content.

A9.11 Regarding the services in scope, our measures apply to AI services – including chatbots – if they are considered user-to-user services under the Act.[472] However, we note that chatbots which do not allow users to share generated content with other users would not meet the definition of a user-to-user service under the Act. We do not have any powers over services if they fall outside the definitions of the kinds of services regulated under the Act.

A9.12 We have separately set out our reasoning for not recommending the measure to regulated search services in chapter 9: Deployment of proactive technology to detect image-based CSAM, in the section entitled 'Who the measure applies to'.

A9.13 We are aware that the Government is planning to introduce illegal harm duties for chatbots and is currently consulting on its proposals.

Testing the proactive technology criteria with the sector

A9.14 Lucy Faithfull Foundation said the principles set out in the proactive technology criteria should undergo thorough testing with the sector to ensure they support detection of known and unknown CSAM, including AI-generated images.[473]

Our response

A9.15 We consider that we have already tested our criteria with the sector to a certain extent. As set out in chapter 9: Deployment of proactive technology to detect image-based CSAM, in the section entitled 'Benefits and effectiveness of the proactive technology criteria and draft guidance', we have developed our criteria by drawing on evidence from relevant

[469] BILETA response to the June 2025 Consultation, p. 2.
[470] Common Sense Media response to the June 2025 Consultation, pp. 6-7.
[471] NSPCC response to the June 2025 Consultation, pp. 31-32.
[472] Section 3(1) of the Act states that a "user-to-user service" means an internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service.
[473] Lucy Faithfull Foundation response to the June 2025 Consultation, p. 4.

existing national and international frameworks on responsible AI and automated content moderation. Further, we have publicly consulted on our criteria and have engaged with stakeholders directly.

Assessments and criteria should be based on outcomes to users

A9.16 Two civil society stakeholders said that proactive technology assessments for accuracy, effectiveness and lack of bias and our criteria should focus on outcomes for users, including meaningful reductions in harm and exposure to harmful content:

- Glitch stated that accuracy in proactive technologies must go beyond statistics and include outcomes broken down by race, gender, sexuality, and other protected characteristics. Further, it stated that effectiveness should not only be measured by the volume of content removed but also by whether survivors are spared re-traumatisation and have meaningful redress, noting reports that images are often taken down but later reappear.[474]
- The Molly Rose Foundation said that Ofcom focuses on process over outcomes in its proactive technology measures, arguing that the criteria emphasised accuracy without addressing the impact on users' exposure to harmful content. It cited its own analysis of Digital Services Act transparency data showing that 98% of moderation decisions were made by just two platforms, suggesting that these criteria appear unlikely to drive effectiveness of proactive technology that is necessary or could be achieved with outcome-focused measures.[475]

Our response

A9.17 We have decided not to recommend that our measures be based on general outcomes and/or impacts to users. As outlined in our December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement) in 'Our approach to developing Codes measures', to recommend an outcomes-based measure we need to be able to identify a sufficiently clear means for a provider to meet that outcome.

A9.18 Understanding the exact causality between how proactive technology is configured and user outcomes is complex and varies across different contexts and services. We therefore consider it would not be possible for us to recommend a sufficiently clear means for providers to meet such a high level outcome in our measures. We explain our reasoning further in chapter 9: Deployment of proactive technology to detect image-based CSAM, in the section entitled 'Our decision'.

A9.19 Regarding Glitch's suggestion that service providers measure beyond statistics, we note that doing so would require significant resource and is not something we consider providers can always undertake in a meaningful way at this time. However, as outlined in our 'Online Safety in 2025' report,[476] we will be monitoring and evaluating the impact of our measures and whether the changes are translating into a safer life online for UK users.

[474] Glitch response to the June 2025 Consultation, p. 5, 11.
[475] Molly Rose Foundation response to the June 2025 Consultation, p. 9, 15.
[476] Ofcom (2025), Online Safety in 2025: A summary of the technology sector's response to the UK's new online safety rules.

External criteria are not compatible with internal metrics

A9.20 Meta Platforms Inc. (Meta) stated that it would be difficult for providers to assess whether external technologies meet the required criteria and noted that, while it uses internal metrics to assess accuracy, external standards may not be a useful way to assess the effectiveness of proactive tools.[477]

Our response

A9.21 We do not agree with Meta's argument. We consider that the measure gives providers flexibility to use their own internal criteria to assess the specified technologies[478] that they choose to deploy, so long as they meet our proactive technology criteria.

Application to file sharing and storage services

A9.22 Three stakeholders requested clarification on the inclusion of all file sharing and storage services in scope, arguing the inclusion of these services may conflict with Ofcom's power to only recommend proactive technology measures to content communicated publicly:

- Microsoft asked for guidance on applying measures to file storage and file sharing services, highlighting uncertainty about how this aligns with scope being on content communicated 'publicly'. It stated this was especially needed given the distinction that may exist in practice between uploading and sharing between services.[479]
- Open Rights Group said file storage was not publication and cited UK GDPR and ICO guidance to argue private cloud storage should be treated as confidential personal data, not subject to proactive scanning. It stated the Act distinguishes between public and private messaging, and that file storage and one-to-one communications are private under Article 8 of the European Convention on Human Rights (ECHR) and data protection law. It warned that the proposals should only apply to public file-sharing and publication, not private storage or messaging.[480]
- European Digital Rights Organisations said they were deeply concerned about Ofcom's proposed obligations requiring file-sharing, file-storage, and user-to-user services to deploy proactive monitoring and hash-matching systems.[481]

Our response

A9.23 As we set out in chapter 8: Introduction to proactive technology, in the section entitled 'Analytical framework for making recommendations regarding the use of proactive technology', the Act is clear that Ofcom is only able to recommend the use of proactive technology for content communicated publicly.[482]

A9.24 Providers should assess whether their service allows for content to be communicated publicly.[483] We consider there may be inputs that are publicly available that the specified

---

[477] Meta Platforms Inc. (Meta) response to the June 2025 Consultation, p. 10.

[478] Specified technologies are classes or sub-classes of technology we have assessed to be in principle accurate, effective and lacking in bias where they meet our proactive technology criteria.

[479] Microsoft response to the June 2025 Consultation, p. 4.

[480] Open Rights Group response to the June 2025 Consultation, pp. 18-19.

[481] European Digital Rights Organisations response to the June 2025 Consultation, p. 1.

[482] Schedule 4 to the Act, paragraph 13(4).

[483] We have set out guidance which is intended to assist services in deciding whether content is communicated 'publicly' or 'privately' for this purpose in Ofcom, 2024. Guidance on content communicated 'publicly' and 'privately' under the Online Safety Act.

technologies we recommend can analyse for the purpose of detecting unknown image-based CSAM. We consider that these providers should adopt the measure for content that is available publicly if their service supports this.

Application to gaming services

A9.25 A member of the Philippine Survivor Network recommended expanding the measure to include online gaming services, which they said are increasingly used for grooming and other forms of child exploitation.[484]

Our response

A9.26 Our Illegal Harms Register of Risks already highlights evidence of gaming services facilitating harms including grooming and wider CSEA.[485] As is the case for all providers of regulated services under the Act, providers of regulated gaming services will need to assess their own risk levels, and where they meet the threshold for being in scope of the measure, they will be expected to act in accordance with the recommended measure.

Application to codes sharing environments

A9.27 One industry stakeholder stated that services hosting unusual categories of user-generated content may face unique moderation challenges. It expressed that the costs that code-sharing environments would face are likely underestimated as they involve complex technical content for which fewer solutions exist, which increases cost of developing or adapting proactive technologies.[486]

Our response

A9.28 We have defined the risk of image-based CSAM as a risk of an offence specified in any of paragraphs 1 to 4, 7, 8 or 10 of Schedule 6 to the Act, so far as the risk in relation to those offences relates to CSAM in the form of photographs, videos or visual images. Where a provider has not identified itself as medium or high risk of image-based CSAM, based on this definition, we do not consider the provider would be in scope of the measure.

[484] A member of the Philippine Survivor Network response to the June 2025 Consultation, pp. 12-13.
[485] Ofcom, 2026. Illegal Harms Register of Risks, p. 61, 65, 70, 71, 72.
[486] GitHub response to the June 2025 Consultation, pp. 3-4.

A10. Hash matching

Further stakeholder responses received on our perceptual hash matching for terrorism content measure by theme

General agreement or disagreement

A10.1 We received support from a range of stakeholders in response to our proposal.[487] We also received several responses that disagreed with our proposal.[488]

Our response

A10.2 We have carefully considered all the feedback received by stakeholders in reaching the decisions set out in chapter 10: Hash matching – Measure on perceptual hash matching for terrorism content.

Effectiveness of perceptual hash matching

Hash matching increases detection

A10.3 Some stakeholders agreed that hash matching increased detection of terrorism content.[489] [✂].[490]

Risk of false positives and false negatives

A10.4 A number of stakeholders noted the risk of false positives within the terror hash matching measure.[491]

A10.5 Several stakeholders raised concerns regarding false negatives.[492] Free Speech Union expressed concerns about technical issues (such as hash collisions[493]), the risk of over removal, and Open Rights Group raised the issue of the lack of published error rates for terrorism hash matching.[494]

---

[487] Commissioner Designate for the Victims of Crime in Northern Ireland response to the June 2025 Consultation, p.5; Department for Justice Northern Ireland response to the June 2025 Consultation, p.11; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.10; Evangelical Alliance response to the June 2025 Consultation, p.7; Information Commission's Office (ICO) response to the June 2025 Consultation, p.15; [✂]; [✂]; Online Safety Network (OS Network) response to the June 2025 Consultation, p.20; [✂]; Tech Against Terrorism response to the June 2025 Consultation, p.5; [✂].

[488] Computer and Communications Industry Association (CCIA) response to the June 2025 Consultation, p.10; Google LLC response to the June 2025 Consultation, p.23; [✂]; Leuthje, Y. response to the June 2025 Consultation, p.5; [✂]; Porter, J. response to the June 2025 Consultation, p.6.; [✂].

[489] [✂]; Tech Against Terrorism response to the June 2025 Consultation, p.4- 5.

[490] [✂].

[491] BILETA response to the June 2025 Consultation, p.16; Open Rights Group Campaign response to the June 2025 Consultation, p.29. [✂]; [✂];[✂]; [✂]; [✂]; [✂]; [✂].

[492] [✂]; Open Rights Group response to the June 2025 Consultation, pp.26 -27; [✂].

[493] A hash collision occurs when two distinct inputs produce the same hash value as output from a hash function. While hash functions are designed to map data of arbitrary size into a fixed-size output (hash values), they are not immune to collisions due to mathematical constraints on the size of their output space. Please see: JumpCloud. What is a hash collision?.

[494] Free Speech Union response to the June 2025 Consultation, p.5; Open Rights Group response to the June 2025 Consultation, p.27.

Our response

A10.6 We maintain that perceptual hash matching is the most appropriate technology for the purpose of this measure. We have put in several safeguards to help mitigate the risk of false positives and false negatives for the measure, including the impact on freedom of expression. These include requiring service providers to ensure their technology strikes an appropriate balance between precision and recall, human review of an appropriate proportion of detected content, and the operation of a user complaints and appeal process.

A10.7 We have added a measure to our content moderation measures in all of the Codes of Practice to ensure that decisions are reversed so far as possible and appropriate where the providers find them to be false positives. An explanation of this measure and our reasoning is available in chapter 9: Deployment of proactive technology to detect image-based child sexual abuse material (CSAM) – Steps to take on reversal of content decisions.

A10.8 This measure aims to mitigate against the risk of false positives. While we are aware that there is a risk of false positives and false negatives, we consider that our provisions in relation to the configuration of the technology help to mitigate these risks. Providers are also likely to be subject to data protection law, the accuracy and fairness principles of which provide an important safeguard against content being erroneously moderated.

Rights impacts

A10.9 We received a variety of feedback from stakeholders related to rights, which we have discussed throughout chapter 10: Hash matching. In addition, we also received feedback from stakeholders on topics which include:

a) UK definition of terrorism and the breadth of the Act;
b) Foreseeability of the measure; and
c) Insufficient safeguards, for example insufficient oversight and ineffective appeals and complaints processes, impacting freedom of expression.

A10.10 We respond to these in turn in the following paragraphs.

UK definition of terrorism and breadth of the Act

A10.11 Several stakeholders provided feedback on the definition of terrorism.[495] Open Rights Group and Microsoft raised the lack of a universal definition for terrorism and lack of international consensus.[496] Open Right Groups noted the potential for broad or uncertain thresholds in identifying illegal content.[497] techUK raised concerns about how services would be expected to determine, with sufficient confidence, whether content or an organisation meets an expanding definition of terrorist content, particularly where the organisation is not designated under UK law.[498]

A10.12 The Commissioner Designate for Victims of Crime Northern Ireland highlighted the specific contextual risks in Northern Ireland, and suggested that service providers should take these into account. It noted that "consideration should be given as to whether such technologies might also be usefully employed in cases where content is shared to

[495] Microsoft response to the June 2025 Consultation, p.6; Open Rights Group Campaign response to the June 2025 Consultation, p.5; Open Rights Group response to the June 2025 Consultation, p.24.
[496] Microsoft response to the June 2025 Consultation, p.6.
[497] Open Rights Group Campaign response to the June 2025 Consultation, p.24
[498] TechUK response to the June 2025 Consultation, p.16.

coordinate attacks on a certain section of the community but not under a specific banner of a proscribed organisation".[499]

Foreseeability of the measure

A10.13 In response to our June 2025 Additional Safety Measures Consultation (June 2025 Consultation), some stakeholders argued that our proposals risked unlawfully restricting freedom of expression by failing to meet legal standards of foreseeability and clarity, citing various pieces of evidence including a legal opinion by Dan Squires KC.[500]

A10.14 As to the foreseeability of the measure's impact on regulated services and users, a legal commentator[501] noted that another proactive technology measure that we consulted on does not specify thresholds for precision or recall or how much detected content should be subject to human review. They argued this raises questions about the foreseeability of the measure.

Insufficient safeguards impacting freedom of expression

A10.15 Stakeholders also argued that without strong oversight, the measure could lead to over-removal of lawful content, with the extent of impact depending on the scale of incorrect identifications.[502]

A10.16 One stakeholder raised concerns about how services were meant to meet this widening definition of terror content. This could lead to the over-removal of content and inadvertently impact legitimate advocacy, journalism, or academic discourse, and may have a chilling effect on freedom of expression — especially in politically sensitive contexts or when content relates to conflict regions.[503] Open Rights Groups noted that automated systems struggle to accurately interpret the nuanced meaning of content, especially when it involves complex or culturally specific contexts. This can result in the over-removal of legitimate content, such as political protests or educational materials.[504]

A10.17 In relation to user appeals, a stakeholders argued that existing complaints and appeals mechanisms may not provide sufficient safeguards where lawful content is wrongly affected, citing the absence of statutory timescales, compensation rights, or independent appeal routes.[505]

Our response

A10.18 In relation to the definition of terrorism and the breadth of the Act, we note stakeholders' concerns regarding the definition of terrorism in UK law and the lack of international consensus on the term. These issues relate to the legislative framework established by Parliament and reflected in the Act. Ofcom's role is to implement that framework and to set out measures that service providers can take to comply with their duties under the Act.

A10.19 We have also considered stakeholders' concerns regarding foreseeability and clarity. As discussed in chapter 10: Hash matching – Measure on perceptual hash matching for

---

[499] Commissioner Designate for the Victims of Crime Northern Ireland response to the June 2025 Consultation, p.6.
[500] Open Rights Group response to the June 2025 Consultation, pp. 24-31; Open Rights Group Campaign response to the June 2025 Consultation, pp.4-5.
[501] Cyberleagle, 2025. Ofcom's proactive technology measures: principles-based or vague?. Similar points were raised in response to our June 2025 Consultation by Open Rights Group, pp.23-26.
[502] BILETA response to the June 2025 Consultation, p.15-16; [✂]; [✂]; [✂].
[503] techUK response to the June 2025 Consultation, p.16.
[504] Open Rights Group response to the June 2025 Consultation, pp. 24-31
[505] Open Rights Group response to the June 2025 Consultation, pp.29-30.

terrorism content, we consider that the measure provides sufficient clarity regarding its scope and operation, while allowing providers flexibility to determine certain implementation details in light of the nature of their service and systems.

A10.20 In relation to insufficient safeguards impacting freedom of expression, we recognise that service providers' appeals processes play an important role in identifying and rectifying false positives. We consider that the Act and our existing Code recommendations secure that appropriate action will be taken in relation to UK users' appeals. To strengthen these safeguards, we have introduced a measure requiring providers to reverse moderation decisions, so far as possible and appropriate, where they determine that content or accounts have been incorrectly actioned. An explanation of this measure and our reasoning is available in chapter 9: Deployment of proactive technology to detect image-based CSAM – Steps to take on reversal of content decisions. We consider that these processes provide an appropriate mechanism for remedying errors and mitigating impacts on lawful expression.

Costs

Cost of hash matching and incorrect moderation

A10.21 Mega indicated that hash matching video content is resource intensive.[506]

A10.22 UK Finance noted that hash matching could incorrectly remove legal content, causing cost, time, reputational damage, and legal risk.[507]

Our response

A10.23 Our impact assessment assumes that a service implements perceptual hashing for images and video without having prior hash matching technologies. Our estimates reflect the higher overall cost to providers of using perceptual hashing instead of cryptographic.

A10.24 The incremental impact of perceptual hashing on some services may be lower if the service already uses perceptual hashing of video for other harms or transcodes video for other purposes, which reduces the difference in cost between perceptual and cryptographic hashing for video.[508] Our assessment accounts for the fact perceptual hashing is more resource-intensive. We explain in chapter 10: Hash matching why we consider it to be more effective than cryptographic hashing.

A10.25 We note the stakeholder feedback on the cost of incorrect moderation. We have covered aspects of this feedback, particularly the impact on freedom of expression and the mitigations we have put in place to mitigate this in chapter 10: Hash matching. We have also recommended a new measure for the purpose of addressing the steps service providers should take on reversal of content decisions. An explanation of this measure and our reasoning is available in chapter 9: Deployment of proactive technology to detect image-based CSAM – Steps to take on reversal of content decisions.

---

[506] Mega response to the June 2025 Consultation, p.18-19.
[507] UK Finance response to the June 2025 Consultation, p.11.
[508] Video perceptual hash matching is generally considered to be more computationally intensive than image hash matching because services will need to decode or transcode video files, extract representative frames, and generate perceptual hashes across multiple points within the video. For services that already do this for other purposes (such as compression of the video, format optimisation, or moderation workflows), the cost to decode or transcode video files may not be a challenge or have any associated cost associated with perceptual hash matching for videos.

Moderator training and cost

A10.26 Stakeholders highlighted that effective moderation of terrorism and violent extremist content requires specialised expertise.[509] techUK noted that the expertise should not be treated as interchangeable with expertise in other content areas such as CSAM.[510] Mega also noted practical challenges in implementing human review with some providers lacking the necessary expertise and therefore relying on alternative mechanisms such as takedown requests.[511]

A10.27 Several stakeholders highlighted the additional costs to providers of having trained moderators.[512] Open Rights Group noted that our cost estimate for moderation was less than the minimum salary of one full-time equivalent worker (FTE).[513]

Our response

A10.28 Measure ICU C7 in our existing Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes) states that providers of large or multi-risk services should ensure that individuals working in content moderation receive training that enable them to fulfil their role in taking down illegal content, including terrorism. Many of the services in scope of this measure will likely be in scope of measure ICU C7 and therefore no additional costs will be incurred.

A10.29 We have also produced guidance for services on making illegal content judgements in chapter 2: Terrorism of our Illegal Content Judgements Guidance, published alongside this statement in full.

A10.30 Our estimate of moderation costs in the section titled 'Impacts and costs' in chapter 10: Hash matching – Measure on perceptual hash matching for terrorism content reflects for a hypothetical service the time a moderator would spend reviewing material flagged by the hash matching system and is less than a full FTE. This represents the proportion of a FTE employee's time spent on this type of content, not how many actual moderators are employed. We assume a provider already employs moderators to comply with existing moderation measures.

Third-party databases

Support for the use of third-party databases

A10.31 Industry and civil society stakeholders provided feedback supporting the use of specific third-party datasets.[514]

Membership criteria for third-party databases

A10.32 UK Finance expressed concerns that small providers might struggle to access third party databases due to strict membership criteria.[515]

---

[509] BILETA response to the June 2025 Consultation, p.17; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.10; [✂]; [✂]; [✂]; Open Rights Group response to the June 2025 Consultation, p.29; TechUK response to the June 2025 Consultation, p.15-17; [✂].
[510] techUK response to the June 2025 Consultation, p.17.
[511] Mega Privacy LLC response to the June 2025 Consultation, pp.24-25.
[512] BILETA response to the June 2025 Consultation, p.17; [✂]; [✂]; []; [✂].
[513] Open Rights Group response to the June 2025 Consultation, p.29.
[514] BILETA response to the June 2025 Consultation, p.18; [✂]; GitHub response to the June 2025 Consultation, p.6; OS Network response to the June 2025 Consultation, p.20; [✂].
[515] UK Finance response to the June 2025 Consultation, p.11.

Availability of a suitable third-party database

A10.33 One stakeholder explained that no existing hash database maps precisely onto the definition in Schedule 5 of the Act, and that requiring datasets to be curated strictly by reference to that statutory scope would be unrealistic and inconsistent with real-world content moderation practice.[516]

Our response

A10.34 We note the stakeholder feedback supporting the use of third-party datasets. In our measure we explain that we now consider there to be at least one third party database, Tech Against Terrorism's hash list API service, that does meet our criteria for an appropriate set of hashes. See annex 4.5: Hash matching for terrorism content: assessment of Tech Against Terrorism's hash list API service.

A10.35 Regarding membership criteria, Tech Against Terrorism's hash list API is an example of a third-party hash list that we consider meets our criteria for an appropriate set of hashes. It does not operate on the basis of membership criteria and is available to services seeking access to the database.

A10.36 Regarding availability of a suitable database, in the consultation we explained that terrorism hash matching should rely on databases containing only hashes of known terrorism content. While we cited GIFCT and TAT as examples of terrorism focused databases, we recognised that both extend beyond UK proscribed organisations and therefore include hashes outside the scope of the terrorism offences under the Act.

A10.37 We accept that no provider currently offers a dataset limited solely to terrorism offences in scope of the Act. However, as an example we are satisfied that a sufficient proportion of TAT's database comprises content amounting to UK terrorism offences and that content which does not amount to a UK terrorism offence is either capable of being filtered out by services or presents a low risk of comprising more than a small proportion of the database. This assessment is set out in annex 4.5: Hash matching for terrorism content: assessment of Tech Against Terrorism content hash list.

Accountability and auditing

A10.38 A number of stakeholders raised concerns about the lack of information regarding audit processes, lack of public oversight and transparency in relation to the audits, and limited public data on third party databases.[517]

Our response

A10.39 There are a range of safeguards in place to ensure that content that is detected as a result of the hashes is illegal, and to provide recourse where content is incorrectly identified as illegal. We have added a measure to our content moderation measures in all of the Codes of Practice to ensure that decisions are reversed so far as possible and appropriate where the providers find them to be false positives. An explanation of this measure and our reasoning is available in chapter 9: Deployment of proactive technology to detect image-based CSAM – Steps to take on reversal of content decisions. We have also set out safeguards for this particular measure, set out in the section titled Rights impact in chapter 10: hashmatching and in annex 4.3: Human review for proactive technology.

---

[516] Tech Against Terrorism response to the June 2025 Consultation, p.5.

[517] BILETA response to the June 2025 Consultation, pp. 15 - 16; Open Rights Group response to the June 2025 Consultation, p.31; [✂]; [✂]; [✂].

Expansion of hash matching to other harms

A10.40 Several stakeholders supported extending the use of hash matching to other harms.[518] The Commissioner Designate for Victims of Crime Northern Ireland stated that consideration should be given as to whether hash matching should be employed in cases where content is shared to coordinate attacks on specific sections of a community but not under the banner of a proscribed organisation.[519] The Antisemitism Policy Trust stated that perceptual hash matching should be extended to other illegal harms, particularly illegal hate.[520] Digital Resilience in Education (Welsh Government) stated that their support for the measure extended to animal abuse content as this may link to terror content.[521]

A10.41 [✂].[522] Two industry stakeholders raised concerns regarding the high cost and resource requirements to implement hash matching for additional harms.[523] The Computer and Communications Industry Association (CCIA) stated that existing hash matching could not be easily expanded to additional harms, as each harm requires its own specialised approach and expertise for effective detection and enforcement.[524]

Our response

A10.42 We note the stakeholder feedback on expanding the use of hash matching to other harms. We are not considering the expansion of hash matching to other illegal harms as part of this statement.

Manuals and written material

A10.43 A stakeholders considered that the measure should include documentation including manuals and manifestos.[525]

Our response

A10.44 We note the stakeholder feedback on manuals and written material. We consider the types of material described by the stakeholders are already in scope of the measure both in terms of the types of content (such as photos, videos or visual materials), and in chapter 2: Terrorism of the Illegal Content Judgements Guidance.

Proactive technology

A10.45 Several stakeholders requested flexibility in the proactive technology used on their service to detect terrorism content. They advocated for changes such as allowing service providers flexibility in deciding how to implement proactive technology and allowing for alternative methods that are most effective for each service.[526]

---

[518] Antisemitism Policy Trust response to the June 2025 Consultation, p.3; Commissioner Designate for the Victims of Crime Northern Ireland response to the June 2025 Consultation, p.5; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.10.
[519] Commissioner Designate for the Victims of Crime Northern Ireland response to the June 2025 Consultation, p.5.
[520] Antisemitism Policy Trust response to the June 2025 Consultation, p.3.
[521] Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.10.
[522] [✂].
[523] Mega response to the June 2025 Consultation, pp 24, and 27; Pinterest response to the June 2025 Consultation, p.4.
[524] Computer and Communications Industry Association (CCIA) response to the June 2025 Consultation, p.10.
[525] Department of Justice for Northern Ireland response to the June 2025 Consultation, p.10.
[526] Computer and Communications Industry Association (CCIA) response to the June 2025 Consultation, p.11; Google LLC response to the June 2025 Consultation, pp.21-22; [✂]; [✂]; [✂]; [✂].

A10.46 Two stakeholders, expressed support for adding terrorism to the proactive technology measure.[527] A government stakeholder expressed this view due to concerns about the scale and nature of the online terrorist threat and encouraging services to take a proactive approach towards disrupting online terrorist activity.[528]

Our response

A10.47 We recognise stakeholder concerns about recommending a single technology rather than a broader principles-based approach, particularly regarding the need for flexibility and innovation. However, this measure does not preclude services from deploying additional or more advanced technologies.

A10.48 We also welcome evidence to help us consider whether or not to recommend the use of other proactive technologies to detect terrorism, as we may turn to this in the future.

Limitations of proactive technology

A10.49 European Digital Rights Organisation stated that content scanning technologies have well known limitations. It argued that hash matching only works for verified content; that AI-based scanning cannot reliably detect context, and that both approaches would lead to false positives and privacy risks while capturing little harmful content.[529]

Our response

A10.50 We note the stakeholder feedback on the limitations of proactive technology. In our June 2025 Consultation we set out how our measure was designed to detect known terrorism content. We have not recommended the use of any artificial intelligence-based scanning as part of the proposed measure. The challenge of false positives and privacy risks have been considered separately in chapter 10: Hash matching. We have also added a measure to our content moderation measures in all of the Codes of Practice to ensure that decisions are reversed so far as possible and appropriate where the providers find them to be false positives. An explanation of this measure and our reasoning is available in chapter 9: Deployment of proactive technology to detect image-based CSAM – Steps to take on reversal of content decisions.

Further stakeholder responses received on our measure on extending perceptual hash matching for child sexual abuse material (CSAM) by theme

Effectiveness in addressing CSAM

A10.51 Multiple stakeholders corroborated our assessment that hash matching is effective to address child sexual abuse material (CSAM) and its associated harms. This included:

- protecting victims and survivors from ongoing traumatisation; [530]
- removing content quickly;[531]

[527] [✂]; [✂].
[528] [✂].
[529] European Digital Rights Organisation response to the June 2025 Consultation, p.1.
[530] A member of the Philippine Survivor Network's response to the June 2025 Additional Safety Measures Consultation (June 2025 Consultation), p.19.
[531] A member of the Philippine Survivor Network's response to the June 2025 Consultation, p.19.

- detecting video-based CSAM;[532]
- protections for "less digitally confident users";[533]
- providing additional protection to women and girls, and aligning with the need to prevent upload of CSAM within high-risk environments;[534]
- identifying children at risk;[535]
- reducing the proliferation of CSAM (and thus disrupting offender pathways), reducing the cycle of offending/recidivism;[536]
- assisting law enforcement in perpetrator disruption and victim safeguarding;[537]
- encouraging reporting and reducing harm;[538] and
- reducing the need for manual review of distressing material.[539]

A10.52 The Association for UK Interactive Entertainment (Ukie) said members recognised hash matching's role in tackling CSAM.[540] The Free Speech Union acknowledged the usefulness of perceptual hash matching and proactive technologies for CSAM and terrorist material but said it retained concerns relating to the risk of hash collisions resulting in over-removal of content, and the reliance of providers on third-party compilers.[541]

A10.53 Google LLC stated that hash matching is particularly effective for CSAM as it does not require added context, and that identification of duplicate content through hash matching allows resources to be applied to previously unseen/unreported content.[542]

A10.54 University College London (UCL) Gender and Tech Research Lab stated that there are gaps in prevention across the ecosystem as it is "currently treated as discretionary rather than mandatory".[543]

Our response

A10.55 We assess that these suggested benefits provide further support for the effectiveness of perceptual hash matching to detect CSAM.

A10.56 We understand there are some concerns about how this measure will be applied. However, after reviewing all the feedback, we consider that these are sufficiently addressed through existing safeguards in the Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes).[544]

---

[532] NSPCC response to the June 2025 Consultation, p.29.
[533] BILETA response to the June 2025 Consultation, p.19.
[534] BILETA response to the June 2025 Consultation, p.18.
[535] [✂].
[536] [✂].
[537] [✂].
[538] [✂].
[539] Scottish Government response to the June 2025 Consultation, p.3.
[540] Association for UK Interactive Entertainment (Ukie) response to the June 2025 Consultation, pp.23-24.
[541] Free Speech Union response to the June 2025 Consultation, p.5.
[542] Google LLC response to the June 2025 Consultation, pp.7-8.
[543] University College London (UCL) Gender and Tech Research Lab response to the June 2025 Consultation, p.2.
[544] Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes), Measure ICU C9.

Providers' existing application of hash matching

A10.57 Some industry stakeholders confirmed in their consultation responses that they currently apply hash matching on their services.[545]

A10.58 techUK stated that many of its members implement hash matching.[546]

A10.59 A range of civil society and an industry stakeholder said that there are existing tools available that are effective to implement perceptual hash matching.[547]

A10.60 The Internet Watch Foundation (IWF) stated that its own hash-matching tool, Image Intercept, is available for smaller providers to implement hash matching through a plug-in.[548] It stated that 5,966 images of CSAM were matched through Image Intercept between 3 July 2025 and 14 October 2025.[549]

Our response

A10.61 The theme supports our assessment of the existing use of hash matching tools and indicates that they are an effective measure used by providers/recommended by civil society organisations.

Pornography services as high-risk

A10.62 An industry stakeholder responded that pornography services are not all necessarily high-risk for image-based CSAM, which would vary by service.[550]

Our response

A10.63 As set out in the section titled 'Effectiveness and benefits' in chapter 10: Hash matching – Extending perceptual hash matching for CSAM, the available evidence base suggests that pornography services are often particularly high risk for the hosting and dissemination of CSAM.

A10.64 Due to this, and because hash matching is highly effective in the detection of CSAM, extending the scope of this measure will result in a material increase in the volume of CSAM that is detected and removed from online services. We expect this, in turn, to deliver material benefits.

Smaller services in-scope of the measure

A10.65 An individual stakeholder and two industry stakeholders challenged the extension of the measure to high-risk pornography services, suggesting it could bring some smaller services into scope.[551]

Our response

A10.66 As set out in the section titled 'Effectiveness and benefits' in chapter 10: Hash matching – Extending perceptual hash matching for CSAM, we explain why pornography services are

---

[545] Friends2Follow response to the June 2025 Consultation, p.6; [✂]; [✂]; [✂].
[546] TechUK response to the June 2025 Consultation, p.18.
[547] A member of the Philippine Survivor Network response to the June 2025 Consultation, pp.19-20; BILETA response to the June 2025 Consultation, p.19; Google LLC response to the June 2025 Consultation, p.7; IWF response to the June 2025 Consultation, pp.31-32; IWF. Image Intercept | Detect & Stop Known Child Sexual Abuse Imagery; NSPCC response to the June 2025 Consultation, p.29.
[548] IWF response to the June 2025 Consultation, p.32.
[549] IWF response to the June 2025 Consultation, p.34.
[550] Hammy Media response to the June 2025 Consultation, p.10.
[551] [✂]; [✂]; [✂].

high risk for CSAM regardless of their size, and how this potential for harm justifies including all services whose primary purpose is hosting or disseminating regulated pornographic content and who are at high risk of image-based CSAM in scope of this measure.[552] We did not receive any new evidence to change this understanding.

A10.67 We note that there are free hash checking services available, such as the Image Intercept tool offered by the IWF, which means that implementation of hash matching should be feasible even for smaller services.[553]

Extension of the measure

A10.68 Some civil society and public body stakeholders recommended that the measure be extended to include all pornography services regardless of their determined level and/or risk of image-based CSAM.[554]

Our response

A10.69 We have taken a risk-based approach to this measure so that our recommendations are proportionate. However, as stated in our Illegal Harms Risk Assessment Guidance, we normally expect all pornography services to be assessed as high risk for CSAM, unless there are strong reasons to assess at a lower risk level.[555]

A10.70 As stated in the December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement), we will continue to keep the scope of this measure under review. Should additional evidence emerge, we are open to considering further extensions subject to being confident that third party providers of hash matching databases have sufficient capacity to support these.

Alternative measures/flexibility

A10.71 Some industry stakeholders stated that there should be flexibility for services in how they can implement the measure/meet the safe harbour.[556]

A10.72 In contrast, the Domestic Abuse Commissioner for England and Wales recommended explicitly stating mandatory tools and standards.[557] Similarly, two stakeholders asked Ofcom to be clear around what is (and is not) considered 'technically feasible' and how services should measure and/or record this, including whether cost should ever be considered as a factor in feasibility.[558] Open Rights Group raised concerns around the level of discretion that providers have over proactive technology measures, potentially leading to differing levels of content removal. It urged Ofcom to set more definite thresholds for e.g. an acceptable level of false positives and how much human review must occur.[559]

---

[552] We also provide further reasoning in the June 2025 Consultation, paragraphs 13.4-13.7.
[553] IWF. Image Intercept | Detect & Stop Known Child Sexual Abuse Imagery.
[554] Barnardo's response to the June 2025 Consultation, pp.11-12; C3P response to the June 2025 Consultation, p.14; Children's Commissioner's Office (CCO) response to the June 2025 Consultation, pp.17-18; Department of Justice for Northern Ireland response to the June 2025 Consultation, p.12; Lucy Faithfull Foundation response to the June 2025 Consultation, p.6; NSPCC response to the June 2025 Consultation, p.29.
[555] Ofcom (2024), Risk Assessment Guidance and Risk Profiles, p.64.
[556] Google LLC response to the June 2025 Consultation, pp.7-8; [✂]; Online Dating and Discovery Association (ODDA) response to the June 2025 Consultation, p.5.
[557] Domestic Abuse Commissioner response to the June 2025 Consultation, p.2.
[558] Online Safety Network (OS Network) response to the June 2025 Consultation, p.20; UCL Gender and Tech Research Lab response to the June 2025 Consultation, p.3.
[559] Open Rights Group response to the June 2025 Consultation, p.27.

A10.73 An industry stakeholder submitted that robust identity and age verification for all uploaders and participants prior to the publication of pornographic content are more effective measures to preventing CSAM compared to hash matching.[560]

A10.74 [✂].[561]

Our response

A10.75 Based on the provisions set out in our Illegal Content Codes measure ICU C9 to manage hash databases, technical configuration, false positives, and human moderation, we assess that the measure retains sufficient flexibility whilst also ensuring that there are appropriate safeguards in place to protect users' rights.[562] [563]

A10.76 We do not consider it appropriate to explicitly name mandatory tools and standards. By not doing so, we enable providers to take a flexible approach that makes the most sense for their service (for example, calibrating precision and recall depending on the number of false positives detected when the technology is deployed).

A10.77 As explained throughout chapter 10: Hash matching, we consider that hash matching is an important tool for detecting and removing CSAM, and is particularly effective at identifying images of post-pubescent children.

Human review

A10.78 Some stakeholders provided feedback related to human review. These related to:

- [✂];[564]
- regular review of human moderation arrangements;[565]
- the "lack of adequate coverage" in existing hash databases and to false positives, which together have required more human review than expected;[566] and
- levels of human review.[567]

Our response

A10.79 We considered this in the December 2024 Statement.[568] The Illegal Content Codes for the existing measures ICU C9.15-9.18 also contain recommendations for human moderation as part of this measure.[569] As set out in chapter 10: Hash matching section titled 'Our decision', we have made some amendments to the factors to which it is appropriate to have regard in determining the appropriate proportion of human review.

A10.80 We assess that concerns around training and supervision are addressed through the existing Illegal Content Code Measure ICU C7 which states that "[t]he provider should

[560] [✂].
[561] [✂].
[562] Illegal Content Codes, Measure ICU C9.
[563] Ofcom (2024), December 2024 Statement, Vol2. Service design and user choice.
[564] [✂].
[565] Domestic Abuse Commissioner response to the June 2025 Consultation, p.2.
[566] Mega Privacy LLC response to the June 2025 Consultation, pp.13, 15.
[567] For example, Open Rights Group suggested that every match from hash matching technology should be subject to human review. See Open Rights Group response to the June 2025 Consultation, p.30.
[568] Ofcom (2024), December 2024 Statement, Vol.2, chapter 4: Automated Content Moderation, p.169-170.
[569] Illegal Content Codes, Measures ICU C9.15-C9.18.

ensure individuals working in content moderation receive training and materials that enable them to fulfil their role in moderating content".[570]

A10.81 In terms of hash databases possibly lacking in adequate coverage,[571] we appreciate that human review can help to mitigate this. However, we consider it a separate matter from whether or not it is appropriate to deploy hash-matching. Hash matching is proven to be an effective way to find known CSAM content. In chapter 9: Deployment of proactive technology to detect image-based CSAM, we set out our conclusion on ways to find unknown CSAM content.

A10.82 We have amended the factors to be taken into account in determining the appropriate proportion of human review to clarify that the level of assurance the provider has in the accuracy of the detection, included by having regard to any further automated processing it carries out, is key. Where a match is within very narrow parameters of being exact, or further automated processing can be used to cross check a match, there may be no need for human review. We have also made it clearer that the harm to victims and those exposed to CSAM content is relevant, as are the impacts on the posting user of false positives.

A10.83 In combination, we assess that this provides sufficient flexibility for providers to apply human review in a way that helps to identify false positives, limit adverse impacts on users' rights, and promote good decision-making.

A10.84 We have decided to issue draft guidance regarding how to apply an appropriate proportion of human review, published alongside this statement.

Hash databases

A10.85 Some respondents noted the reliance of the measure on underlying hash databases. This included:

- the reliance of the measure on underlying third party hash databases, which they said can ary in quality, this included the potential for inaccuracy, such as false positives and subsequent user frustration;[572]
- variation in quality of databases;[573]
- the suitability of different content types for first- or third-party solutions;[574]
- the lack of coverage in existing hash databases;[575]
- the difficulty in maintaining up-to-date databases;[576]
- the need for strong security measures around hash matching systems;[577] and
- reliance on third-party hashes potentially causing over-blocking due to quality issues.[578]

[570] Illegal Content Codes, Measure ICU C7.
[571] Mega Privacy LLC response to the June 2025 Consultation, pp.13-16.
[572] Middle Tech Coalition response to the June 2025 Consultation, p.4.
[573] Google LLC response to the June 2025 Consultation, p.7.
[574] Google LLC response to the June 2025 Consultation, p.7.
[575] Mega Privacy LLC response to the June 2025 Consultation, p.11.
[576] Integrity Institute response to the June 2025 Consultation, p.5.
[577] UCL Gender and Tech Research Lab response to the June 2025 Consultation, pp.2-3.
[578] Free Speech Union response to the June 2025 Consultation, p.5.

A10.86 UCL Gender and Tech Research Lab suggested that Ofcom should centrally consolidate hash lists.[579] The National Center for Missing & Exploited Children (NCMEC) flagged the hash-sharing initiatives it facilitates, which it considered would support compliance with the proposal.[580]

Our response

A10.87 In the Illegal Content Codes (ICU C9.7-ICU C9.11), we set out recommendations for providers to ensure that the set of hashes that providers are using is appropriate for the measure.[581]

A10.88 We consider that the principles set out in the December 2024 Statement provide sufficient assurance that the database(s) used will support an effective use of hash matching and gives guidance to support service providers in sourcing an appropriate database.

A10.89 We refer to our position in the December 2024 Statement, paragraph 4.97: "This measure allows service providers the flexibility to choose a third-party database of CSAM hashes. […] Recommending a centralised organisation would limit the ability of service providers to choose a database for their services."[582]

False positives

A10.90 Some stakeholders suggested the hash matching measure is prone to or would lead to false positives.[583] Specific concerns were:

- the potential for false positives due to the nature of online adult services;[584]
- incorrect or conflicting classifications, incorrect submissions, technical issues, and lack of verification;[585]
- associated business commercial and reputational risk;[586]
- due to hash matching remaining a developing technology with efficacy of data bases still being tested, rushed implementation could result in excessive content removal and false positives;[587]
- a precision rate for CSAM detection that is lower than that for terrorist content;[588]
- the technical risk of hash collisions that could cause over-removal;[589] and
- the need for regular review of technical parameters.[590]

---

[579] UCL Gender and Tech Research Lab response to the June 2025 Consultation, p.2.
[580] National Center for Missing & Exploited Children (NCMEC) response to the June 2025 Consultation, p.6.
[581] Illegal Content Codes, Measures ICU C9.7-ICU C9.11.
[582] Ofcom (2024), December 2024 Statement, Vol.2, chapter 4: Automated content moderation, p.174.
[583] European Digital Rights Organisations response to the June 2025 Consultation, p.1; [✂].
[584] Name Withheld 4 response to the June 2025 Consultation, pp.5-7. This stakeholder also referred to research that they said showed perceptual hash matching algorithms show false positives and false negatives. Having reviewed these, we consider them to be limited in relevance to CSAM detection, and as such the findings of these pieces of research do not sufficiently change our position on pursuing this extension.
[585] Mega Privacy LLC response to the June 2025 Consultation, pp.10-11.
[586] Mega Privacy LLC response to the June 2025 Consultation, pp.10-11.
[587] Middle Tech Coalition response to the June 2025 Consultation, p.4.
[588] Tech against Terrorism response to the June 2025 Consultation, p.8.
[589] Free Speech Union response to the June 2025 Consultation, p.5. The response noted this was rare with high-quality algorithms.
[590] Domestic Abuse Commissioner response to the June 2025 Consultation, p.2.

Our response

A10.91 Our Illegal Content Codes measure ICU C9.8 b) sets out several safeguards designed to minimise false positives and ensure that they are managed by providers in a rights-preserving way. Provisions set out in ICU C9.8 b), e) and f) help to prevent incorrect material being used in a hash database, mitigating this potential source of false positive. ICU C9.12 also sets out principles for the technical configuration of the technology.[591]

A10.92 On the issue of adult services, we understand that the potential similarity in appearance between legitimate adult content and CSAM may lead to an increased likelihood of false positives. This is due to a potential structural/visual similarity to the known source images (in this case adult content and CSAM). It is dependent upon the distance metric used; the wider the distance metric, the more likely this will be.

A10.93 However, we have set out a number of principles to assist in technical configuration, and our assessment remains the same as outlined in paragraph 4.129 of our December 2024 Statement: "if hash matching is implemented in accordance with the safeguards we have set out, it should have a very high level of accuracy and give rise to relatively small numbers of false positives."[592] [593]

A10.94 As set out above, we have been clear that the appropriate proportion of human review depends on the level of assurance in the correctness of the detection outcomes of the provider's processes. A provider using wide perceptual matching parameters, or whose quality assurance processes were detecting unexpected false positives, would need to increase the human review it carried out of matches.

A10.95 As such, we propose no further changes to the measure.

Hash matching alone is not sufficient

A10.96 Some stakeholders stated that hash matching was not enough to address the issue of online CSAM and additional measures/steps were needed to complement the use of hash matching.[594]

A10.97 Barnardo's, European Digital Rights Organisations, [✂], the Scottish Government and [✂] stressed that hash matching can only detect known/reported CSAM.[595] The Integrity Institute noted that hash matching does not capture all harmful content, as it can be evaded.[596]

A10.98 Stakeholders suggested additional measures to complement the use of hash matching, including:

- measures requiring providers to respond quickly when content is reported;[597]

---

[591] We discuss the issue of false positives in further detail in Ofcom (2024), December 2024 Statement, Vol.2, chapter 4: Automated content moderation, p.181-183.
[592] We recognise that the level of false positives could initially be higher where hash matching is first implemented on a service, as technical parameters and human review policies are adjusted.
[593] Ofcom (2024), December 2024 Statement, Vol.2, chapter 4: Automated content moderation, p.182.
[594] Barnardo's response to the June 2025 Consultation, p.8; European Digital Rights Organisations response to the June 2025 Consultation, p.1; [✂]; Integrity Institute response to the June 2025 Consultation, p.5; Scottish Government response to the June 2025 Consultation, p.3; [✂].
[595] Barnardo's response to the June 2025 Consultation, p.8; European Digital Rights Organisations response to the June 2025 Consultation, p.1; [✂]; Scottish Government response to the June 2025 Consultation, p.3; [✂].
[596] Integrity Institute response to the June 2025 Consultation, p.5.
[597] Scottish Government response to the June 2025 Consultation, p.3.

- deterrence messaging;[598]
- recommender system intervention and livestream mitigations;[599]
- identity verification of uploaders and performers (specific to pornographic content);[600]
- future-proofing the measure to tackle unknown CSAM, including AI-generated content;[601] and
- requiring hash matching for pornographic content itself.[602]

Our response

A10.99 Some of our existing and proposed measures also correspond to the suggestions from stakeholders, including swift content take-down, recommender systems measures and detection of unknown CSAM. We refer to the relevant Illegal Content and Protection of Children Codes for details of measures relevant to this feedback.

A10.100 We encourage providers to go further than what is recommended in our measures, if they can do so, in order to offer further mitigations against the harm caused by image-based CSAM.

Feedback on our cost assessment

A10.101 [✂] and Ukie highlighted the additional cost of specialist staff and system upgrades needed to make a hash matching system operationally functional.[603]

A10.102 [✂] said that our impact assessment neglected cost factors such as auditing, operational, and social costs.[604]

A10.103 One individual disagreed with the impact assessment and considered the costs infeasible for smaller providers.[605]

A10.104 Middle Tech Coalition and Pinterest said that Ofcom's cost assessments were underestimated.[606] A third stakeholder, Ukie, estimated that it would take six to nine months to implement the measure including testing and certification.[607]

A10.105 Mega Privacy LLC said that the overall cost of developing its CSAM hash matching system was much higher than Ofcom's estimates because of challenges with end-to-end encryption. It also stated that the video processing costs to carry out perceptual hash matching on video are extremely high, including the resource required to transcode the video into compatible formats and apply the hashing process at scale.[608]

---

[598] IWF response to the June 2025 Consultation, pp.31-32; Lucy Faithfull Foundation response to the June 2025 Consultation, pp.6-7; UCL Gender and Tech Research Lab response to the June 2025 Consultation, p.3.
[599] UCL Gender and Tech Research Lab response to the June 2025 Consultation, p.2.
[600] Hammy Media Ltd response to the June 2025 Consultation, p.10.
[601] Barnardo's response to the June 2025 Consultation, p.8; Integrity Institute response to the June 2025 Consultation, pp.4-5; IWF response to the June 2025 Consultation, pp.33-36; Scottish Government response to the June 2025 Consultation, p.3.
[602] Domestic Abuse Commissioner response to the June 2025 Consultation, pp.4-5. The response also noted that older teen girls were highly vulnerable but had fewer safeguards than younger peers.
[603] [✂]; Ukie response to the June 2025 Consultation, p.28.
[604] [✂].
[605] Name Withheld 9 response to the June 2025 Consultation, p.9.
[606] Middle Tech Coalition response to the June 2025 Consultation, p.4; Pinterest response to the June 2025 Consultation, p.5.
[607] Ukie response to the June 2025 Consultation, p.28.
[608] Mega Privacy LLC response to the June 2025 Consultation, pp.9-10; pp.16-17.

Our response

A10.106 Our December 2024 Statement outlined additional detail on how we estimated the costs of moderation associated with this measure and gave illustrative costs for services of given sizes and risk levels.[609]

A10.107 Auditing and operational costs are included within our maintenance cost estimates.[610] Social costs, including the measure's interference with users' rights to freedom of expression (which we consider is limited given the safeguards we have in place) are discussed in more detail in the 'Risk' and 'Rights Impacts' sections of the December 2024 Statement.[611]

A10.108 Our cost estimates have a wide range to reflect that services of different sizes and complexity would incur different costs. The wage and time assumptions underlying our estimates are consistent with Ukie's estimation.[612]

Rights impact

A10.109 Some respondents raised concerns relating to how the proposed measure could restrict people's freedom of expression.

- The Free Speech Union and Porter, J. considered that the measure could lead to adverse impacts on freedom of expression due to excessive removal of content.[613]
- [✂].[614]
- [✂].[615]
- Open Rights Group considered that Ofcom has not sufficiently evidenced how its proposals meet its duties under the Human Rights Act 1998 and Equality and Human Rights Commission (EHCR). It stated that content being blocked by means of proactive technology unlawfully restricts users' right to express and receive that information, thereby limiting their freedom of expression.[616]

A10.110 European Digital Rights Organisations considered that the measure would impose a general monitoring obligation which is prohibited under European Union (EU) law. It also submitted that hash matching only detects known content and that it will lead to false positives. Furthermore, it said that broad monitoring would capture very little harmful content while exposing all users to privacy risks.[617]

---

[609] Ofcom (2024), December 2024 Statement, Vol.2: The causes and impacts of online harms, paragraph 4.111-4.114; Annex 5: Assumptions on costs and further analysis on costs and benefits, paragraphs A4.30-A4.36.
[610] See chapter 10: Hash matching – Extending perceptual hash matching for CSAM, Table 10.2: Estimated costs to service providers of implementing hash matching for CSAM.
[611] Ofcom (2024), December 2024 Statement, Vol.2, chapter 4: Automated content moderation.
[612] Ukie response to the June 2025 Consultation, p.28.
[613] Free Speech Union response to the June 2025 Consultation, p.5; Porter, J. response to the June 2025 Consultation, p.2.
[614] [✂].
[615] [✂].
[616] Open Rights Group response to the June 2025 Consultation, pp.24-30.
[617] European Digital Rights Organisations response to the June 2025 Consultation, p.1.

Our response

A10.111 We do not consider that our decision to extend the measure changes our prior assessment of the freedom of expression impacts and privacy impacts of the measure, which is set out in the December 2024 Statement.[618]

Other feedback

A10.112 [✂].[619]

A10.113 European Digital Rights Organisations responded that private communications may be affected by the measure.[620]

Our response

A10.114 We consider that our previous assessment of the effectiveness of hash matching in comparison to human moderation alone is sufficient to support an automated approach where technically feasible. We also consider that preventative approaches and reactive approaches complement each other in the design of online services to ensure that they are as safe as possible for users.

A10.115 We are explicit that the measure applies only to content communicated publicly. Providers may choose to deploy proactive technology across privately communicated content if they decide to do so, if it is technically feasible for them to do so, and so long as they comply with data protection law. However, this is their own commercial choice. As set out in chapter 8: Introduction to proactive technology, our Codes of Practice may not recommend the use of proactive technology for content communicated privately.

[618] Ofcom (2024), December 2024 Statement, Vol.2, chapter 4: Automated Content Moderation.
[619] [✂].
[620] European Digital Rights Organisations response to the June 2025 Consultation, p.1.

A11. Recommender systems

Further stakeholder responses received on this chapter by theme

A11.1 This section outlines further stakeholder feedback on our proposed recommender systems measure and our response to these remarks.

Comments on measure scope

Inclusion of fraud in measure

A11.2 Several stakeholders suggested that the measure should be expanded to include either fraud; financial service offences; scams; fraudulent advertising and paid-for content; and/or money laundering.[621] Some of these stakeholders provided case studies and other pieces of evidence to demonstrate how recommender systems can lead to the systematic amplification of fraudulent content or other financial harm.[622] UK Finance noted the complexity of accurately detecting fraud content online and considered that this is a reason to include fraud within scope of the measure. It also said that recommender systems might prioritise scam content due the use of high-engagement tactics such as urgent or emotional language, which may encourage engagement-based ranking models to include them in users' feeds.[623]

A11.3 The National Crime Agency/National Economic Crime Centre (NCA/NECC) suggested this measure should also include services at high risk of malicious advertising.[624]

Our response

A11.4 Whilst stakeholders have provided evidence demonstrating that users encounter fraudulent content via content recommender systems, we do not consider that this sufficiently demonstrates the exponential or virulent nature of these harms in *children's* recommender feeds in the same manner as we consider still exists for hate, terrorism, suicide and self-harm. In light of our decision to limit the application of the measures to children's recommender feeds, we do not consider it proportionate to expand the measures to fraud.

A11.5 Under the Online Safety Act 2023 (the Act), the Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes) can only address user-generated content. As such, paid-for advertisements are not in scope of these measures.[625] In relation to fraudulent

[621] Financial Conduct Authority (FCA) response to the June 2025 Consultation, pp.3-4; [✂]; [✂]; [✂]; UK Finance response to the June 2025 Consultation, pp.12-13; We Are Survivors response to the June 2025 Consultation, pp.7-8; Which? response to the June 2025 Consultation, pp.11-12.
[622] FCA response to the June 2025 Consultation, pp. 3-4; [✂]; Which? response to the June 2025 Consultation, pp.11-12.
[623] UK Finance response to the June 2025 Consultation, pp.12-13.
[624] NCA response to the June 2025 Consultation, pp.16-18.
[625] An advertisement is a "paid-for advertisement" in relation to an internet service if the provider of the service receives any consideration (monetary or non-monetary) for the advertisement (whether directly from the advertiser or indirectly from another person), and the placement of the advertisement is determined by systems or processes that are agreed between the parties entering into the contract relating to the advertisement. See s236 of the Online Safety Act 2023 (the Act).

advertising, see our July 2026 Consultation on draft Fraudulent Advertising Codes of Practice.[626]

Inclusion of intimate image abuse (IIA) and child sexual abuse material (CSAM) in the scope of the measure

A11.6 Several charities and civil society organisations suggested the measure be expanded to include non-consensual intimate imagery (NCII) and/or child sexual abuse material (CSAM).[627] The NSPCC provided an evidentiary case study as to how recommender systems can facilitate the dissemination of CSAM, as well as identifying that accounts selling CSAM can benefit from algorithmic amplification.[628]

Our response

A11.7 We have recommended a suite of various measures specifically aimed at targeting child sexual exploitation and abuse (CSEA) and CSAM, which are better suited to the issues identified by these stakeholders. This includes our IIA hashing measure (ICU C14), which came into force 30 September 2026, as well as our CSAM hashing measure (ICU C9) and Proactive technology to detect image-based CSAM measure (ICU PT1).[629]

A11.8 Accounts which benefit from algorithmic amplification do so as a result of network recommender systems, whereas these measures only apply to content recommender systems. We acknowledge the risk highlighted by NSPCC in the Illegal Harms Register of Risks (Illegal Harms Register), whereby network recommender systems can facilitate NCII/IIA or CSAM dissemination. Addressing harms in network recommender systems requires distinct measures from those we have confirmed here or elsewhere.

A11.9 We consider that our existing measures on grooming help to address some of the risk highlighted by the NSPCC in relation to the amplification of specific user accounts. In our Illegal Content Codes, we recommend that in-scope services ensure child user accounts have network expansion prompts switched off by default, and that child users do not appear in the network expansion prompts of adult users.[630] This is part of a suite of default settings that aim to make it harder for offenders to find and communicate with child users.

A11.10 Overall, we do not consider it proportionate to recommend inclusion of these harms in these measures at this time.

Measure should include other harms, harm areas, and/or content

A11.11 Some stakeholders suggested variously that the measure should include other harms or harm areas such as self-harm; extreme pornography; harassment; extremist radicalisation content; animal cruelty; and/or legal but harmful content (especially for children).[631] Glitch said that the measure framed 'harm' as largely individual content violating individual categories and failed to account for intersectional harms such as anti-Black misogyny

---

[626] Ofcom (2026), July 2026 Consultation, Fraudulent Advertising Codes of Practice.
[627] National Society for the Prevention of Cruelty to Children (NSPCC) response to the June 2025 Consultation, pp.30-31; Online Safety Network (OS Network) response to the June 2025 Consultation, pp.22-24; Refuge response to the June 2025 Consultation, pp.13-14.
[628] NSPCC response to the June 2025 Consultation, pp.30-31.
[629] Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes), Measure ICU C9.
[630] Illegal Content Codes, Measure ICU F1.
[631] 5Rights response to the June 2025 Consultation, p.10; Barnardo's response to the June 2025 Consultation, pp.13-14; Glitch response to the June 2025 Consultation, pp. 14-18; [✂]; Molly Rose Foundation response to the June 2025 Consultation; pp.7-16; NSPCC response to the June 2025 Consultation, pp.30-31; Samaritans response to the June 2025 Consultation, p.8; Social Media Animal Cruelty Coalition (SMACC) response to the June 2025 Consultation, pp.12-13.

('misogynoir') and gender-expansive abuse, as well as for collective behaviour (such as coordinated abuse of individuals).[632]

A11.12 By contrast, one respondent said that terrorism content should not be within Ofcom's scope and that only the security services should be responsible for detecting and responding to terrorism content online.[633]

A11.13 [✂].[634]

A11.14 Three civil society organisations urged Ofcom to require platforms to limit the spread of content which itself is not illegal content, but is used to promote and advertise content that is (such as CSAM and/or adult content).[635] CARE noted that many adult users used social media platforms to market their adult content available on other platforms, and that this marketing material is readily available to children.[636]

A11.15 Glitch said that recommender systems mainly work in English and misread multilingual UK communities. It recommended measurable Language Coverage and Parity Standards, demonstrating minimum precision and recall across the top languages used in UK online spaces, and for dialects or hybrid forms.[637]

Our response

A11.16 While we acknowledge that some stakeholders have suggested the inclusion of additional harms and/or content, we either did not have sufficient evidence as to the systematic risk posed by content recommender systems to include them, or we consider the harms are already addressed under our Protection of Children recommender systems measures PCU E1 and E2.[638] [639] [640]

A11.17 Overall, we do not consider it proportionate to include these harms within scope of these measures at this time.

---

[632] Glitch response to the June 2025 Consultation, pp.12-15.
[633] Porter, J. response to the June 2025 Consultation, p.1.
[634] [✂].
[635] 5Rights Foundation response to the June 2025 Consultation, p.11; Christian Action Research and Education (CARE) response to the June 2025 Consultation, pp.2-4; OS Network response to the June 2025 Consultation, p.23.
[636] CARE response to the June 2025 Consultation, pp.2-4.
[637] Glitch response to the June 2025 Consultation, p.13.
[638] Primary priority content refers to pornographic content, and content which encourages, promotes, or provides instructions for suicide; self-harm; or an eating disorder or behaviours associated with an eating disorder.
[639] Priority content refers to content that is abusive on the basis of race, religion, sex, sexual orientation, disability or gender reassignment; content that incites hatred against people on the basis of race, religion, sex, sexual orientation, disability or gender reassignment; content that encourages, promotes, or provides instructions for serious violence against a person; bullying content; content which depicts serious violence against (or graphically depicts serious injury to) a person or animal (whether real or fictional); content that encourages, promotes, or provides instructions for stunts and challenges that are highly likely to result in serious injury; and content that encourages the self-administration of harmful substances.
[640] Non-designated content refers to content, which is not primary priority content or priority content, of a kind which presents a material risk of significant harm to an appreciable number of children in the UK.

Expand to network recommender systems

A11.18 Some organisations said that the measure should be extended to network recommender systems to address the harm posed by accounts who regularly share illegal content. Stakeholders named a range of additional harms, variously noting CSAM and [✂].[641]

Our response

A11.19 We have taken steps to address the risk of network recommender systems in relation to grooming. In our Illegal Content Codes, we recommend that in-scope services ensure child user accounts have network expansion prompts switched off by default, and that child users do not appear in the network expansion prompts of adult users.[642] This is part of a suite of default settings that aim to make it harder for offenders to find and communicate with child users.

A11.20 In addition, we consider that where users have regularly posted demonstrably illegal content, this would constitute relevant available information as described in paragraph 11.47c of chapter 11: Recommender systems. This would mean that we expect providers to take information like users' violative posting history into account when considering if content is indicated to be potentially illegal content, and whether or not to exclude it from children's recommender feeds. Please also see chapter 3: User sanctions of this statement, where we are recommending additional measures which address how providers should have regard to users who repeatedly post illegal content in their user sanctions policy.

A11.21 Overall, however, network recommender systems are a distinct technology to content recommender systems, and achieving a similar policy intent here would require a separate measure. We will keep this under review.

Overly negative or inaccurate portrayal of content recommender systems

A11.22 One provider raised concerns with Ofcom's portrayal of content recommender systems, which they considered to be "inherently problematic".[643]

A11.23 Dr Kira, B. considered that our proposed measure misdiagnosed the issue it was seeking to mitigate, due to a flawed understanding of recommender systems themselves. Dr Kira, B further described recommender systems as content-agnostic engagement machines and stated that Ofcom's proposal could be read as an argument for services demoting content from these recommender systems, rather than outright removing it.[644]

A11.24 Google LLC considered that recommender systems play an important role in how services maintain a responsible platform, including by connecting young users with age-appropriate content. It said that changing how content recommender systems work based on potential illegality could negatively impact the user experience, leading to more irrelevant and/or lower-quality content being promoted to users.[645]

---

[641] 5Rights Foundation response to the June 2025 Consultation, pp.10-11; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.11; [✂]; OS Network response to the June 2025 Consultation, pp.22-24.
[642] Illegal Content Codes, Measure ICU F1.2.
[643] [✂].
[644] Dr Kira, B. response to the June 2025 Consultation, pp.6-10.
[645] Google LLC response to the June 2025 Consultation, pp.26-28.

Our response

A11.25 We recognise the positive impact these functions can have on the user experience, such as providing users with content that may be of greater interest to them. We have reiterated such positive impacts in paragraphs 11.1 in chapter 11: Recommender systems. We have also acknowledged recommender systems will vary service to service in chapter 11: Recommender systems.

A11.26 Despite these positive impacts, however, we also consider content recommender systems to introduce users to risk of harm as identified in the Illegal Harms Register, as demonstrated in chapter 11: Recommender systems.

A11.27 We have a duty to respond to the risk of harm to users with proportionate measures, and we consider the risk of harm outlined in the chapter and supported by independent evidence to warrant appropriate measures in response.

Compliance issues

A11.28 A number of civil society organisations and charities made various points regarding provider compliance with the measure and our enforcement of this measure.[646]

Our response

A11.29 We have a variety of tools and methods to ensure compliance with the Act.[647] Our Supervision Team has established relationships with the largest and riskiest service providers to ensure they understand our expectations and can come into compliance quickly. Where we become aware of instances of non-compliance, we have the powers to take enforcement action.

Additional transparency and user control mechanisms

A11.30 Several stakeholders were in favour of additional mechanisms to ensure the effectiveness of the recommender systems measure and to improve users' understanding of their recommender systems. They suggested variously that platforms should provide more public information about how their algorithms work; that platforms should disclose the main parameters of their recommender algorithms, including input data and weightings; [✂]; that platforms should provide relevant parties (e.g. researchers and regulators) improved access to data; and that platforms should introduce the option for users to reset their recommender algorithms.[648]

A11.31 Stakeholders also submitted some proposals for how to improve user control over recommender systems, such as that platforms offer users alternatives to recommender

[646] 5Rights Foundation response to the June 2025 Consultation, pp.10-11; British and Irish Law Education and Technology Association (BILETA) response to the June 2025 Consultation, p.19; Centre for Countering Digital Hate (CCDH) response to the June 2025 Consultation, p.2; Commissioner Designate for Victims of Crime Northern Ireland response to the June 2025 Consultation, pp.6-7; Molly Rose Foundation response to the June 2025 Consultation, pp.15-16; [✂].

[647] Ofcom (2024), Online Safety Enforcement Guidance.

[648] Are, C response to the June 2025 Consultation on Additional Safety Measures, p.17; Demos response to the June 2025 Consultation, pp.2-8; [✂]; Dr. Kira, B response to the June 2025 Consultation, p.9; Open Rights Group response to the June 2025 Consultation, p.32.

algorithms to users; and that platforms should introduce the option for users to reset their recommender algorithms.[649]

Our response

A11.32 We acknowledge the points regarding necessary transparency and providing users control mechanisms. We will keep this under review while we develop our transparency notices for providers.

Comments on measure effectiveness

A11.33 Three organisations and one individual provided various arguments to suggest the measure may not be effective, and/or that it may undermine or overwhelm existing systems of content removal, enforcement and/or appeals.[650]

Our response

A11.34 We consider that we have provided various arguments that demonstrate the measure's effectiveness in principle, especially with regard to the risk of harm it seeks to mitigate.

A11.35 Furthermore, we reiterate that content can be "indicated to be potentially illegal" without triggering the duty for services to moderate that content, meaning providers will not necessarily need to moderate all excluded content. We therefore do not consider that these measures will undermine existing systems and processes.

A11.36 We also consider the flexibility afforded to service providers, through the use of 'relevant available information' used to determine potential illegality, will improve the efficacy of the measure. By relying on all the information a service has available to it, providers can consider potential illegality in a manner that would be more difficult for bad actors to identify workarounds for, or to identify areas for malicious reporting.

Issues specific to livestreaming

A11.37 Two organisations and an individual said that the measure would have a disproportionate effect on recommended livestreams, and therefore also on livestreaming services. This is because such content loses relevance if not watched in real-time, and reinstated recordings of such content would therefore not constitute a suitable mitigation.[651]

A11.38 Twitch said that, as a livestreaming service, it has different functionality to social networking sites or other user-to-user services, and as such has an inherently different risk profile with regard to the spread of illegal content on the service.[652]

A11.39 The British and Irish Law Education Technology Association (BILETA) said it welcomed that livestreams determined to contain illegal content would no longer be recommended to users, but expressed concern that content may be captured before it has been determined to be illegal. It referenced an incident where suicide-related content had been captured from a livestream across multiple platforms, and although the livestream itself had been taken down, 'fixed' content from the livestream remained on many platforms. It said it

[649] Demos response to the June 2025 Consultation, p.7; UK Finance response to the June 2025 Consultation, pp.12-13.
[650] Google LLC response to the June 2025 Consultation, p.4; [✂]; [✂]; [✂]; [✂].
[651] Dr Are, C. response to the June 2025 Consultation, pp. 15-17; Open Rights Group response to the June 2025 Consultation, pp.31-36; [✂].
[652] Twitch response to the June 2025 Consultation, pp.19-22.

would be beneficial to provide guidance on how services are expected to mitigate instances like this in the future.[653]

Our response

A11.40 We consider that the immense risk of harm to children from livestreams containing content amounting to relevant offences, means that it is proportionate for livestreams to be within scope of the measures, even where providers have existing systems and processes for the moderation of livestreams.

A11.41 As providers will be able to rely on a variety of examples of relevant available information to exclude recommended livestreams, we consider this should also reduce erroneous content removals.

A11.42 Additionally, we consider that where livestreamed content is added to the moderation queue, providers are strongly incentivised to moderate it quickly. This is because the live nature of the content compounds any harm, and because livestreamed content is often typically affiliated with user monetisation; and therefore valuable to the provider to promote in feeds. Where content is 'captured' from a livestream and where the provider has reason to suspect it may be illegal content, that content should be reviewed, assessed and (where appropriate) taken down in line with our content moderation measures (ICU C1 and ICU C2)

Measure should be more safety by design or upstream

A11.43 A number of civil society organisations suggested variously that the measure was too reactive, and/or that the measure should focus more on 'upstream' risk mitigation such as proactive systems and service design.[654]

Our response

A11.44 These measures are part of a suite of existing and additional measures that will help to ensure user safety across services and throughout user journeys on these services. The design of these measures – by relying on the innate design and functionality of recommender systems – in our view represents a safety-by-design approach that will reduce children's exposure to relevant illegal content very early in the user experience. This is because it functions before content moderation or other means of reducing user exposure to this kind of content.

A11.45 It would be a significantly greater interference with the rights of both users and providers, to recommend that engagement-driven recommender systems not be used at all.

Definitional clarity

A11.46 Some stakeholders suggested that some of the terms used as part of the proposed measure, such as 'foreign interference offence', 'relevant available information', and/or 'suspected illegal content', were not clearly defined or understood.[655]

---

[653] BILETA response to the June 2025 Consultation, p.23.
[654] 5Rights Foundation response to the June 2025 Consultation, pp.10-11; Antisemitism Policy Trust response to the June 2025 Consultation, p.3; Integrity Institute response to the June 2025 Consultation, pp.7-8; Molly Rose Foundation response to the June 2025 Consultation, pp.3-16; OS Network response to the June 2025 Consultation, pp.22-24; Refuge response to the June 2025 Consultation, pp.13-14.
[655] [✂]; [✂]; Luethje, Y. response to the June 2025 Consultation, p.12; [✂]; We Are Survivors response to the June 2025 Consultation, pp.7-8.

Our response

A11.47 We have addressed more specific conceptual and definitional issues in chapter 11: Recommender systems, under the 'Benefits and effectiveness' section.

A11.48 We would like to clarify that the definition for the 'foreign interference offence' is provided in the Act and is not something we are able to change or reinterpret. Given that the foreign interference offence has been removed from the scope of the measure, we consider that these comments are no longer relevant for the purposes of this measure.

Content violation assessments

A11.49 A number of stakeholders provided evidence relating to how service providers monitor content that was recommended but later found to be violative.[656]

Our response

A11.50 We consider that it is technically feasible (and already carried out by some service providers, as evidenced by some of the respondents) to use various forms of metrics to monitor whether recommended content was violative following its recommendation to users.

Additional guidance for services

A11.51 Some stakeholders suggested that Ofcom should provide further guidance and/or examples of good practice to support service providers in implementing and using automated content identification tool.[657]

Our response

A11.52 We have sought to provide further clarity on how the measures should be applied in chapter 11: Recommender systems.

Comments on proportionality

A11.53 Several stakeholders disagreed with our assessment of the proportionality of the proposed measure.[658] Furthermore, some respondents suggested that the measure may have a disproportionate impact on smaller services.[659] BILETA said that the cost of the measure could bring smaller services to reduce their offerings to users and/or withdrawing from the market entirely, which in turn could lead to further market concentration and less competition.[660]

A11.54 By contrast, other stakeholders suggested that the measure should be applied to a greater range of services.[661] In particular, Molly Rose Foundation urged Ofcom to apply recommender feed exclusions for illegal content to all services, not just those at medium or high risk.[662]

---

[656] Check My Ads response to the June 2025 Consultation, pp.9-10; Evangelical Alliance UK response to the June 2025 Consultation, p.7; [✂].
[657] Antisemitism Policy Trust response to the June 2025 Consultation, p.3; Demos response to the June 2025 Consultation, pp.2-8; [✂]; UK Finance response to the June 2025 Consultation, pp.12-13; [✂].
[658] Computer and Communications Industry Association (CCIA) response to the June 2025 Consultation, pp.12-13; [✂]; [✂]; [✂].
[659] ACT – The App Association response to the June 2025 Consultation, p.8; [✂].
[660] BILETA response to the June 2025 Consultation, p.19.
[661] Molly Rose Foundation response to the June 2025 Consultation, pp.7-16; [✂].
[662] Molly Rose Foundation response to the June 2025 Consultation, pp.7-16.

Our response

A11.55 As set out in the Risk Profiles, services with content recommender systems are likely to have increased risk of hate, terrorism or suicide and self-harm.[663] Services with content recommender systems are only expected to pose a low risk for the relevant harms if there are significant countervailing factors which reduce their risk levels.

A11.56 We recognise the potential impact on smaller services. However, the measures are targeted at services with medium or high risk of relevant serious harms, and do not apply to services that are low risk. We therefore consider that even where these measures are applied to small services they are delivering significant benefits for children.

A11.57 In addition, providers can implement alternative measures to those outlined in chapter 11: Recommender systems, if they achieve the same results. Where they take alternative measures, service providers must also maintain a record of what they have done and how they consider that it meets the relevant duties, including how they have complied with the duty to have particular regard to the importance of protecting freedom of expression and privacy.

A11.58 Overall, we consider it appropriate to recommend these measures for such services and do not consider it necessary to revise our assessment of the measures' proportionality.

[663] Ofcom (2024), Risk Assessment Guidance and Risk Profiles.

A12. Amendment to the Illegal Content Judgements Guidance (ICJG) for CSAM

Further stakeholder responses to the amendment by theme

Problems identifying illegal CSAM content

A12.1 The National Police Chiefs Council (NPCC) stated that technology exists that can "interpret, priorities (sic) and triage" coded harmful content but that it is "not routinely available to policing" and is often only employed in niche cases post-offender disruption.[664]

Our response

A12.2 We appreciate the difficulties for providers and law enforcement agencies in detecting obfuscated and coded language. We consider that our content moderation measures address this concern in part, including the recommendation for service providers to ensure moderators are adequately trained. Regarding the availability of this type of technology in policing, this is a matter for law enforcement rather than Ofcom.

Removing content without reporting it as CSAM

A12.3 The National Crime Agency (NCA) raised concerns that service providers, based on these signals, may not have enough confidence to remove content without seeing it, or may remove the material without reporting as CSAM.[665]

Our response

A12.4 We note the concern that providers may remove CSAM without reporting it. We do however note that section 66 of the Online Safety Act 2023 (the Act) sets out duties for providers to report detected child sexual exploitation and abuse (CSEA) content which is not otherwise reported to the National Crime Agency (NCA). Providers may also have additional CSEA reporting duties in other jurisdictions or have voluntary reporting arrangements. For the avoidance of doubt, this duty applies to any content which amounts to a CSEA offence, including conspiracy to commit CSEA offences and linking to or directing a user to CSAM. Reporting CSAM is dealt with in chapter 3: User sanctions.

Feedback on niche perpetrator knowledge

A12.5 The Canadian Centre for Child Protection (C3P) suggested a broader approach towards what is covered by "explicitly indicates that the contents are CSAM" and "strongly associated with CSAM".[666] [667] It suggested the following examples drawn from its own

[664] National Police Chiefs' Council (NPCC) response to the June 2025 Additional Safety Measures Consultation (June 2025 Consultation), p.6.
[665] The National Crime Agency (NCA) response to the June 2025 Consultation, p.13.
[666] The Canadian Centre for Child Protection (C3P) is a Canadian national charity dedicated to the personal safety of children who also produce resources and research to understand and identify child sexual abuse.
[667] June 2025 Consultation, p.125.

experience – niche offender knowledge such as a CSAM victim or survivor's real name or the name of a popular CSAM series, clothed images of children, and non-CSAM images of CSAM victims or survivors.[668]

Our response

A12.6 We consider that these examples of survivor-related content strongly associated with CSAM as described by C3P (with the exception of clothed images of children which we discuss further in paragraph A12.7) may, when considered in combination with other coded terms containing CSAM, a user complaint and at least one other piece of reasonably available information described in scenario three, strengthen the basis on which a provider can reasonably infer CSAM is present in messages, a group chat or forum.[669]

A12.7 Regarding stakeholder feedback concerning clothed images of children, we consider that using a clothed image of a child, without wider context, is too broad a category to be relied on as reasonably available information given their wide legitimate uses and resulting impacts on freedom of expression and privacy. However, where a clothed image of a child is identified through sources, such as CSAM hash databases or established keyword lists, as forming part of, or appearing in, a known CSAM series, we consider that it may be treated as reasonably available information under scenario three. Where this cannot reasonably be known by the provider, we do not consider that the image should be relied on as an indicator.

A12.8 We have decided not to include CSAM victims or survivors' names in users' account names or bio text as a piece of additional information that can be used to infer illegality. This decision reflects the significant risk of false positives with regard to the use of survivors and victims of CSAM's real names. We do not consider the presence of a CSAM survivor or victims' name in a username or bio text to be reasonable grounds to infer illegality, even when in combination with other pieces of reasonably available information.

Alternative or additional measures

A12.9 A number of stakeholders from civil society, industry, and members of the public suggested alternative or additional measures alongside the guidance.

- In terms of content moderation processes, [✂].[670]
- Open Rights Group suggested that providers suspend access to a chat pending further investigation, rather than removing content straight away. It stated this would ensure investigation and prosecution, preserve any evidence, and protect against wrongful takedown.[671]
- The Online Safety Network (OS Network) emphasised the need for providers to share reported data (which we assume means connected content) with moderation teams to enable assessment of illegality, which some providers already do.[672]

---

[668] C3P response to the June 2025 Consultation, p.11-12.
[669] 'Survivor-related content' refers to any material that may identify a victim or survivor, such as their name, and depict images that may not be classified as CSAM, however, they are images adjacent to the abuse images themselves.
[670] [✂].
[671] Open Rights Group response to the June 2025 Consultation, p.22.
[672] The Online Safety Network response to the June 2025 Consultation, p.26.

- The UK Association for Interactive Entertainment (Ukie) suggested we should instead focus on evidence-sharing with law enforcement, improve intelligence flows, and support voluntary use of detection systems if it is proportionate to the risk and technically feasible. It highlighted this in reference to "compliant low risk sectors such as video games".[673]
- In respect to the guidance itself, Ukie recommended that we maintain a flexible approach to allow for measures to be put in place that meet "equivalent safety outcomes".[674]
- [✂]. A stakeholder suggested the first scenario be reworked to "adopt a risk-based, context-sensitive framework" which allows providers to apply the "most appropriate" measures based on the context of the violation.[675]

Our response

A12.10 We thank stakeholders for their alternative proposals. To include any further measures in this iteration of the Illegal Content Codes of Practice for user-to-user services (Illegal Content Codes), we would need to carry out additional impact assessments and a further consultation similar to the process that had informed this statement. We do not consider this to be necessary at this time. We were also not presented with substantive evidence that has changed our assessment of the amendment and guidance following our June 2025 Additional Safety Measures Consultation, or that would suggest that any additional measure would be proportionate and beneficial based on the available evidence.

A12.11 We will consider whether any future legislative changes require updates to our current position and will consult before making any such changes as appropriate.

A12.12 Furthermore, we emphasise that providers may put additional protections in place should they choose to, but this does not call our current proposed guidance into question. Under scenario one, providers would become aware of illegal content and as such are under duties to remove it swiftly and report it to the NCA or another international reporting body, and take other actions as set out within the Codes. Providers may put additional measures in place or take additional steps if they wish to.

A12.13 Regarding Open Rights Group's response, Section 10 of the Act imposes duties on providers to minimise the length of time illegal content is present, and to swiftly take it down once they are aware of it. We have assessed that if a service provider has reasonable grounds to infer from other content (that is technically feasible to review) that the content in question is illegal, the required action is to take down the content. A recommendation to suspend access to a chat rather than remove it or ban the user would be a matter to be addressed in the Illegal Content Codes. We recognise that this may be appropriate in circumstances where a provider did not yet have reasonable grounds to infer the existence of a conspiracy to commit CSAM offences, but did have grounds to be concerned. However, we consider that a suspension obligation is impracticable due to the potential length of an investigation, and the requirement this would cause for providers to maintain suspended chats indefinitely.

A12.14 We also consider this measure does not put additional duties on providers outside of what is already recommended in the Illegal Content Codes. If low-risk providers identify a risk

[673] Ukie response to the June 2025 Consultation, p.25.
[674] Ukie response to the June 2025 Consultation, p.24.
[675] [✂].

that their service may host illegal content, they should review their risk assessment. Otherwise, they should take action against illegal content when they become aware of it in accordance with their illegal content safety duties.

Other risks

A12.15 We are Survivors questioned how proactive technology will adapt to meet changes in perpetrator tradecraft, such as language or signals used.[676]

A12.16 [✂].[677]

Our response

A12.17 In response to the first point, we appreciate that perpetrator behaviour can change quickly, and there is a need for providers to update their moderation processes to reflect this. In terms of this guidance, we consider that, where applicable, measure ICU C7 around supplying adequate training to moderators will mean that moderators stay up-to-date on evolving tradecraft.

A12.18 In response to the second point, providers are required to meet their illegal content safety duties by removing illegal content swiftly when they become aware of it. We consider that the content moderation measures in the existing Illegal Content Codes and in this statement will assist in detecting this content to enable its removal.

Impacts and costs

A12.19 Some stakeholders provided feedback that related to the potential costs and impacts of the guidance, including expressing agreement with our assessment of the impacts associated with the proposal.[678] In particular, the Evangelical Alliance suggested the amendment was low cost, proportionate and privacy preserving.[679]

A12.20 We also received feedback from other stakeholders on our assessment of the impacts of the guidance, who expressed concerns about the costs of implementing it.[680] Ukie did not agree the costs were proportionate, particularly for low risk providers. It stated that 'inference-based judgements' would be a significant resource burden for these services.[681] Snap, Inc. also suggested that estimating the costs of implementing the proposal was not currently feasible.[682] Integrity Institute stated identifying a still of a known CSAM video can only be met if the service integrates databases of known CSAM, which comes with associated risks of false positives, resource demand and overheads.[683]

A12.21 Lastly, the British and Irish Law Education and Technology Association (BILETA) suggested that the incremental costs of updating legal guidance to assist in using hash matching tools to address illegal content is "justifiable and manageable".[684]

---

[676] We are Survivors response to the June 2025 Consultation, p.5.
[677] [✂].
[678] A member of the Philippine Survivor Network response to the June 2025 Consultation, p.17; Evangelical Alliance response to the June 2025 Consultation, p.6; IWF response to the June 2025 Consultation, p.9; [✂].
[679] Evangelical Alliance response to the June 2025 Consultation, p.6.
[680] [✂].
[681] Ukie response to the June 2025 Consultation, p.24.
[682] Snap, Inc. response to the June 2025 Consultation, p.8.
[683] Integrity Institute response to the June 2025 Consultation, p.5.

Our response

A12.22 We do not expect this guidance to add significant resource burdens in addition to the potential impacts set out as part of a provider's content moderation processes. Instead, it should assist providers in making content judgements of content that is already detected. If this leads to an increase in CSEA being detected on a service, we appreciate this may cause a potential increase in costs relating to illegal content reporting to the NCA or another international reporting organisation. However, providers are required under the Act to report CSEA content and therefore these costs are necessary to achieve what is required by the Act. Based on this assessment, we consider that the costs of implementing the proposal is proportionate.

A12.23 The ICJG cannot ask providers to implement content detection technology. However, where we have recommended in Codes that providers adopt content detection technology, we consider it follows that the data such technologies rely on or create is reasonably available information for the purposes of making judgements about the harms concerned.

A13. Combined impact assessment

Further stakeholder responses received on this chapter by theme

Proportionality and evidence

A13.1 Some respondents disagreed with our approach to recommending measures to low risk platforms, noting the need for a diverse digital ecosystem in the UK. They claimed that our approach was disproportionate and lacked sufficient evidence of its effectiveness.[685]

Our response

A13.2 The Online Safety Act 2023 (the Act) requires Ofcom to consider the proportionality of the measures we recommend for different kinds and sizes of services and to providers of differing sizes and capacities and consider the findings of risk assessments.[686] We have followed the directive set in the Act and therefore targeted the more costly measures at larger and/or more risky services.

Technology

A13.3 Some responses raised concerns about the recommendation of specific types of technology and supported a technology-neutral approach in our measures.[687]

Our response

A13.4 Providers have the flexibility to take the approach that best suits their service's context, operating model, and the nature of technology by reference to the risks identified in their risk assessment.

Measuring the impact of the measures

A13.5 UK Finance suggested there needs to be a measurement of impact of the recommended measures on illegal content.[688]

A13.6 One response raised concerns about excessive enforcement and the potentially harmful impact this could have on online communities.[689]

Our response

A13.7 We continue to monitor and evaluate the impact of the measures in our Codes of Practice. Any disclosable results will be published in due course.

A13.8 Ofcom has considered the impact on different groups in annex 2: Equality Impact Assessment and Welsh Language Assessment. Enforcement of the measures will be in line with our Online Safety Enforcement Guidance.[690]

---

[685] GitHub response to the June 2025 Additional Safety Measures Consultation (June 2025 Consultation), p.11; [✂]; [✂].
[686] Paragraph 2 of schedule 4 of the Act.
[687] [✂]; [✂]; Online Dating and Discovery Association (ODDA) response to the June 2025 Additional Safety Measures Consultation, pp.10-11.
[688] UK Finance response to the June 2025 Additional Safety Measures Consultation pp.17-18.
[689] [✂].
[690] Ofcom (2024), Online Safety Enforcement Guidance.

Other responses

A13.9 One respondent said the proposed measures were prescriptive instead of outcome-based, which reduced flexibility for service providers to use existing approaches such as Pan-European Game Information (PEGI) ratings.[691]

Our response

A13.10 We consider our measures to be non-prescriptive where possible, and to give providers flexibility in how they are implemented. We also consider our measures do not directly conflict with other legal frameworks.

[691] Association for UK Interactive Entertainment (Ukie) response to the June 2025 Additional Safety Measures Consultation, pp.41-42.