Illegal Harms updates

New priority offences: serious self-harm and cyberflashing

Statement

Published 25 June 2026

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

Contents

Section

1. Overview 3

2. Introduction 5

3. Stakeholder responses and our decisions 10

4. Next steps 33

Annex

A1. Legal framework 34

A2. Statutory tests and impact assessments 38

1. Overview

1.1 Ofcom is the United Kingdom's communications regulator, overseeing sectors including telecommunications, post, broadcast TV and radio. Under the Online Safety Act 2023 ('the Act'), Ofcom is also the UK regulator for online safety. Under the Act, Ofcom's job is to make online services safer for the people who use them, especially children. Providers of regulated online services ('providers') are required to have effective systems in place to protect all users from illegal content and children from content harmful to children.

1.2 In December 2025, the government created two new 'priority offences' under the Act: encouraging or assisting serious self-harm ('self-harm offence'), and cyberflashing. Both were previously non-priority offences under the Act. Providers have specific duties under the Act in relation to the priority offences.

1.3 In March 2026, we consulted on our proposed changes to the Illegal Harms regulatory documents and guidance (March 2026 Consultation).[1] We explained that in some instances these updates are required by the Act, while in others we have discretion in terms of how we update our regulatory documents and guidance to cover the new priority offences. We are setting out our decisions in this statement after considering all responses to our consultation.

1.4 These decisions will have implications for how providers carry out their illegal content risk assessments and in turn the safety measures that they should adopt to manage and mitigate the risks of harm identified. For more information see section 4 'keeping illegal content risk assessments up to date'.

1.5 We did not consult on new Codes measures associated with these new priority offences. We expect to update our regulatory documents and guidance again in due course to respond to further legislative changes, technological developments and new evidence of illegal content.

What we have decided – in brief

Encouraging or assisting serious self-harm

- We have confirmed our proposal to combine the offence of encouraging or assisting suicide and the encouraging or assisting serious self-harm offence into a single kind of illegal harm. We have updated the Risk Assessment Guidance and the Illegal Content Codes of Practice ('Codes') to reflect this.
- We have confirmed our proposal to update the User-to-User Risk Profile to include the risk factors most strongly associated with suicide and self-harm and added a reference to self-harm to the Search Risk Profile.
- We have updated the Register of Risks suicide and self-harm chapter to include additional evidence on how these harms manifest online, including research on AI chatbots and further evidence on messaging functionalities.
- We have confirmed our proposal to update the Codes to apply existing measures, where relevant, to self-harm in the same way as to the other kinds of illegal harm.

[1] Ofcom, 2026. Consultation: New priority offences - serious self-harm and cyberflashing

- We have confirmed that as a result of combining suicide and self-harm, measures that specifically apply to suicide content or services at risk of suicide should also apply to self-harm content and relevant services at risk of self-harm.
- To reflect the priority status of the serious self-harm offence and our decision to combine suicide and self-harm, we have combined the guidance and annexes on these two offences in one section. We have kept the definition of the two offences separate to reflect that they are separate offences.

Cyberflashing

- We have confirmed our proposal to include cyberflashing as a new, and separate kind of illegal harm. We have updated the Risk Assessment Guidance and Codes to reflect this.
- We have confirmed our proposal to update the User-to-User Risk Profile to include the risk factors most strongly associated with cyberflashing.
- We have confirmed limited updates to the cyberflashing sections of the Register of Risks and Illegal Content Judgements Guidance.
- We have confirmed our proposal to update the Codes to apply existing measures, where relevant, to cyberflashing in the same way the other kinds of illegal harm.
- We have confirmed our proposal to apply the measure relating to blocking and muting (ICU J1) to relevant services at risk of cyberflashing.

What this means for services

- Providers of regulated services must review and update their illegal content risk assessments, to assess the risks of the new kinds of illegal harm on their service. Providers need to assess both suicide and self-harm and assign one overall risk level for 'suicide and self-harm'.
- Providers also need to separately risk assess for cyberflashing and assign a risk level for this harm.
- Updates to the User-to-User and Search Risk Profiles to include risk factors most strongly associated cyberflashing and suicide and self-harm amount to a significant change to the Risk Profiles, meaning providers need to update their risk assessments. Providers need to consider the risk factors in the Risk Profiles when assessing the risks of suicide and self-harm and cyberflashing content on their service.
- Providers with the relevant risks and characteristics should apply the measures recommended in the Codes to mitigate the risks of suicide and self-harm and cyberflashing or take alternative effective measures to manage these risks.[2]

We set out the full detail of our decisions and what this means for services in the following sections of this document.

[2] As explained in this statement, some of the measures which are relevant to the new priority illegal harms are subject to consultation. We have not yet reached final decisions on these consultations.

2. Introduction

Overview of Illegal Harms

2.1 The Act gives service providers a range of duties in relation to illegal content. These duties require providers to assess and manage the risks arising from the offences specified in the Act. Below we set out an overview of the main duties in the Act and the provisions which are particularly relevant to the decisions in this statement. For more information, please see annex 1, Legal framework and refer to our December 2024 Illegal Harms Statement (December 2024 Statement) and accompanying regulatory documents and guidance.

2.2 It is for government and parliament to determine the scope of offences captured by the Act. When government updates the offences in scope, Ofcom is required to consult on corresponding updates to the regulatory framework, including relevant products and guidance, to ensure that providers are able to comply with their duties. This is a statutory requirement and not a matter of discretion for Ofcom.

Illegal content

2.3 The Act defines illegal content as "content that amounts to a relevant offence".[3] The Act sets out the relevant offences in UK criminal law that amount to illegal content.

2.4 The Act lists a number of 'priority offences', which are the most serious offences covered by the Act. In total there are over 130 priority offences in scope of the Act. We previously grouped these into 17 kinds of illegal harms for the purposes of providers' risk assessments and the Codes.[4] In this statement, we are confirming that this will become 18 kinds of illegal harm, including 'suicide and self-harm' (previously 'suicide') and 'cyberflashing'.

Duties on regulated services

2.5 The Act places duties on both user-to-user and search services to assess and manage the risks of harm from illegal content. The nature and scope of these duties, including differences between whether the service is a user-to-user[5] or search[6] service, and between priority and non-priority offences, are set out fully in our December 2024 statement.

2.6 In summary, providers are required to:

a) Carry out and keep up to date illegal content risk assessments; and
b) Implement proportionate measures to mitigate risks and protect users from encountering illegal content.

[3] Section 59(2) of the Act.
[4] We group the offences differently in the Register of Risks and ICJG because of the different purposes of these documents.
[5] A user-to-user service is 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.
[6] A search service is a service that is, or includes, a search engine, which allows users to search more than one website or database.

Duties on Ofcom

2.7 Under the Act, we have duties to produce regulatory documents and guidance to assist providers in complying with their duties.[7] These documents include:

- **Risk Assessment Guidance** – this aims to help providers comply with the illegal content risk assessment duties. The purpose of the risk assessment is to improve providers' understanding of how risks of different kinds of illegal harm could arise on their services, and the safety measures they need to put in place to protect users. It is compulsory for providers to complete an illegal content risk assessment to meet their duties under the Act. The guidance recommends a four-step methodology providers can follow to carry out their risk assessments.
- **Risk Profiles** – these are resources for providers to consult when conducting their risk assessments. Service providers must take account of the relevant Risk Profile (either user-to-user or search) when conducting their risk assessments. The Risk Profiles are made up of a list of risk factors that our Register of Risks indicates are most strongly linked to a risk of one or more kinds of illegal harm. The Risk Profiles help providers to understand which kinds of illegal harm are most likely to occur on their services, and which risk factors may play a role. The Risk Profiles are published as part of the Risk Assessment Guidance.
- **Register of Risks** – the Register is our evidence-based assessment of the causes and impacts of illegal harms based on the evidence that we have gathered. It presents our full risk assessment of where and how illegal harms manifest online and the characteristics of services that are relevant to the risks of harm. It forms part of our duty under the Act to assess the factors that can cause a risk of harm to individuals on a service. It is intended to act as a central resource for service providers when they are conducting their risk assessments. The risk factors identified in the Register of Risks also inform the Risk Profiles, helping service providers identify the areas of greatest likely risk due to particular characteristics in the design, functionality and user base of their services.
- **Illegal Content Judgements Guidance ('ICJG')** – the ICJG is Ofcom's guidance to support service providers in assessing whether content is illegal content for the purpose of complying with their duties under the Act. It is intended to serve as a resource for providers when carrying out their risk assessments and applying measures to mitigate the risks they identify.
- **Illegal Content Codes of Practice ('Codes')** – the Codes set out recommended measures that providers can take to comply with their illegal content safety duties and their reporting and complaints duties under the Act. While providers are not required to adopt the measures recommended in the Codes, providers that do so will be treated as compliant with the duties to which they relate.[8]
- **Record-Keeping and Review Guidance** – this Guidance assists providers with complying with their duties to keep records of their risk assessments and the measures taken to comply with their duties under the Act.

[7] Ofcom, Online safety regulatory documents and guidance
[8] Section 49(1) of the Act.

2.8 We published our final decisions on all these documents as part of our December 2024 Statement.[9] The illegal content safety duties and Codes came into force in March 2025.[10]

Introduction to the new priority offences

2.9 In this section we provide a brief overview of the new priority offences and the harm they can cause.

Encouraging or assisting serious self-harm

2.10 The self-harm offence takes place where a person does an act capable of intentionally encouraging or assisting the serious self-harm of another person.[11]

2.11 The impact on users from encountering illegal self-harm content can be severe. Impacts can be both physical and psychological, and include long-term mental health concerns, eating disorders, physical harm to oneself, and death.

2.12 Research demonstrates a clear association between exposure to self-harm content and a worsening of mood or mental health, and in the most serious cases an increased likelihood of self-harm or suicidal behaviour. Repeated exposure to self-harm content within online communities contributes to the normalisation of self-harm as an acceptable coping mechanism. Research also identifies a contagion effect, whereby viewing self-harm content increases the likelihood of imitation, particularly in environments where graphic imagery or peer endorsement is present.[12]

2.13 Specific content that covers eating disorders could be considered illegal under the offence where it assists or encourages harmful behaviours.

2.14 While most content related to self-harm does not amount to the offence of encouraging or assisting serious self-harm, all content related to self-harm is extremely sensitive and may have the potential to cause harm to users. This is particularly the case for children who, under the Act, should also be protected from content that does not amount to illegal self-harm content, but "encourages, promotes or provides instructions for an act of deliberate self-injury" as well as eating disorder content.[13] While some users who post self-harm and eating disorder content intend to cause harm to others, other users may share this content to find supportive communities, to express their own experiences and connect with those with similar experiences, or to attempt to help others. An explanation of what may

[9] Ofcom (2024), December 2024 Statement. The current versions of these documents are set out on the Ofcom website.

[10] Since then, Ofcom has published further statements setting out decisions to amend these Codes: Ofcom, May 2026,Detecting intimate image abuse and Ofcom, June 2026, Crisis response protocol. The draft amendments are being published separately. Their implementation will be subject to parliamentary process, and the amendments will come into force once this process is completed (the draft amendments relating to detecting intimate image abuse were published on 1 June 2026 and have been laid before Parliament).

[11] Section 184 of the Act.

[12] Ofcom (2024) Register of Risks p.371.

[13] Under the Act, children should be protected from encountering content which encourages, promotes, or provides instructions for self-harm. For more information, see Ofcom's April 2025 Protection of Children Statement
('April 2025 Statement').

constitute harmful content to children and what constitutes recovery content is set out in the Guidance on Content Harmful to Children.[14]

2.15 We set out more detail about how illegal self-harm content manifests online and its impact on users in our updated Register of Risks chapter 'Encouraging or assisting suicide (or attempted suicide), and serious self-harm'.[15]

Cyberflashing

2.16 The offence of cyberflashing is committed where a person intentionally sends a photograph or film of genitals for the purposes of causing alarm, distress or humiliation or for the purpose of obtaining sexual gratification.[16]

2.17 Cyberflashing is a manifestation of existing patterns of sexual violence and abuse which breaches the privacy and sexual autonomy of the victim.[17] Evidence shows that while the impact of cyberflashing is varied and individual, it can have negative psychological impacts. Survivors and victims describe the experience of cyberflashing as aggressive, intimidating and violating. Survivors and victims of cyberflashing also describe feelings of shame, embarrassment and vulnerability following the experience.[18]

2.18 Cyberflashing is a gendered offence, with evidence showing women are nearly three times more likely than men to experience cyberflashing.[19] Evidence also suggests that women in minority ethnic groups and LGBTQ+ groups are disproportionately targeted by cyberflashing.[20]

2.19 Cyberflashing can form part of a pattern of harmful behaviour, with some individuals receiving several images a day.[21] Cyberflashing can co-occur with several other online harms includes stalking, harassment and coercive or controlling behaviour as well as other forms of image-based sexual abuse such as intimate image abuse and extreme pornography.

2.20 We set out more detail about how cyberflashing manifests online and its impact on users in our updated Register of Risks section 'Cyberflashing'.[22]

---

[14] Ofcom (2024) Guidance on content harmful to children p.24.
[15] Ofcom (2026), Updated Register of Risks, pp.117-184.
[16] Section 66A of the Sexual Offences Act 2003.
[17] McGlynn, C. response to 2020 Law Commission Consultation [accessed 2 February 2026]; McGlynn, C. and Johnson, K., 2022. Cyberflashing: Recognising Harms, Reforming Laws. Bristol: Bristol University Press. [accessed 21 September 2023].
[18] Law Commission, 2021. Modernising Communications Offences: A final report [accessed 2 February 2026].
[19] Vera-Gray, F., McGlynn, C., Lovett, J. and Butterby, V., 2026. Freedom under threat. [accessed 2nd June 2026].
[20] McGlynn, C., 2021. Written evidence submitted by Professor Clare McGlynn, Durham Law School, Durham University [accessed 2 February 2026]; McGlynn, C. and Johnson, K., 2022. Cyberflashing: Recognising Harms, Reforming Laws [accessed 2 February 2026].
[21] Revealing Reality, 2023. Anti-social Media: The violent, sexual and illegal content children are viewing on one of their most popular apps. [accessed 26 July 2023].
[22] Ofcom (2026), Updated Register of Risks. pp.361-369.

Structure of this document and accompanying regulatory documents

2.21 Section 3 of this document sets out the decisions we have made to update the Illegal Harms regulatory documents and guidance to reflect the new priority offences. It includes our reasoning and the evidence we rely on to support those changes. In Section 4 we discuss next steps following this statement.

2.22 Alongside this statement, we have published updated versions of the following documents:

- The Risk Assessment Guidance and Risk Profiles;
- The Illegal Harms Register of Risks;
- The ICJG; and
- The Record Keeping and Review Guidance.

2.23 The amendments to the Codes will be implemented separately. We have published draft consolidated versions of the relevant Codes incorporating the draft amendments that Ofcom intends to submit to the Secretary of State.

2.24 Their implementation will be subject to parliamentary process, and the amendments will come into force once this process is completed. We will provide updates on the timing of this process.

2.25 In the March 2026 Consultation, the proposed updates to the Codes included draft amendments to the user control measures and new additional safety measures, which were proposed in the April 2025 Illegal Harms Consultation on User Controls (April 2025 Consultation) and the June 2025 Additional Safety Measures Consultation (June 2025 Consultation) respectively. We explained the impact of the March 2026 proposals, taking into account these additional measures and amendments.[23] We have not yet reached final decisions on the majority of the proposals set out in the April 2025 and June 2025 Consultations.[24] This statement therefore focuses solely on the changes proposed in the March 2026 Consultation.

2.26 We expect to publish our decisions on the amendments to the user control measures proposed in our April 2025 Consultation and the remaining additional safety measures proposed in our June 2025 Consultation in autumn 2026.

[23] The measures in the April 2025 Consultation and June 2025 Consultation which would apply to suicide and self-harm are blocking and muting (ICU J1), disabling comments (ICU J2), reporting imminent harm in livestreams (ICU D17), availability of human moderators for livestreams (ICU C16), proactive technology (ICU C11 and ICU C12), recommender systems (ICU E2); and for cyberflashing, blocking and muting (ICU J1).
[24] The decisions made so far can be found in further statements: Ofcom, May 2026,Detecting intimate image abuse and Ofcom, June 2026, Crisis response protocol.

3. Stakeholder responses and our decisions

3.1 This section sets out stakeholder responses to the March 2026 consultation and our final decisions. We received 16 responses. We have only responded in detail in this statement to the feedback relating to proposed changes to the Illegal Harms regulatory documents and guidance.

3.2 In reaching our decisions, we have carefully considered all responses to the March 2026 Consultation. However, we have not addressed all feedback in detail in this statement, either where it falls outside the scope of what we consulted on or where we have already responded in previous statements and our position remains unchanged.

3.3 In this section, we first consider stakeholder feedback on our overall approach and cross-cutting issues, before considering each of the regulatory products in turn.

Overall approach and cross-cutting issues

Our proposals

3.4 We proposed updates across the Illegal Harms regulatory documents to reflect the fact that the self-harm and cyberflashing offences have now been designated as 'priority offences' by the government.[25] We proposed to combine the new priority self-harm offence with encouraging or assisting suicide to create a single kind of illegal harm, 'suicide and self-harm'. We proposed to include cyberflashing as a new, and separate, kind of illegal harm.

3.5 We proposed to update the Register of Risks with new evidence on self-harm and cyberflashing, and to update the User-to-User Risk Profile to include risk factors most strongly associated with suicide and self-harm and with cyberflashing. We also proposed to introduce a reference to self-harm in the Search Risk Profile.

3.6 Additionally, we proposed to update the Illegal Content Codes of Practice to ensure existing measures apply to cyberflashing and suicide and self-harm in the same way as to other priority illegal harms where relevant, and to extend certain measures to the new priority illegal harms. We did not propose any changes to the substance of the measures in the Codes. We explain our proposals in more detail below.

3.7 As we explain at paragraph 2.25, the March 2026 Consultation also included draft amendments to a number of Codes measures that have been proposed in other online safety consultations. However, we have not yet reached final decisions on the majority of those proposals. This statement therefore focuses solely on the changes proposed in the March 2026 Consultation.

[25] The Online Safety Act 2003 (Priority Offences) (Amendment) Regulations 2025 amends the list of priority offences in Schedule 7 of the Act.

Stakeholder feedback and our decision

Impact of changes

Stakeholder feedback

3.8 Several stakeholders expressed concerns with the position we set out in the consultation that our proposals would not have a significant impact on service providers[26] or users,[27] with one civil society stakeholder adding that this contrasts with the government's ambition of more significant changes to the online ecosystem.[28]

3.9 South West Grid for Learning, End Violence Against Women Coalition and Iris Anticipa called for additional Code measures to tackle cyberflashing.[29]

3.10 Centre for Protecting Women Online expressed concern that we have underestimated the impact of these harms and called for their severity to be reflected in the impact assessment more clearly.[30]

Our decision

3.11 We have decided to confirm the changes we proposed in the March 2026 Consultation. We have decided to combine the offence of encouraging or assisting suicide and the encouraging or assisting serious self-harm offence into a single kind of illegal harm (we discuss this further below), and include cyberflashing as a new, and separate, kind of illegal harm.[31]

3.12 We remain of the view that the changes to the Illegal Harms regulatory products will have a significant impact on user safety. Taken together, these updates form a package that strengthens protections for users from the risks of harm arising from suicide and self-harm and cyberflashing. They are designed to improve how services identify, assess and mitigate risks, and to support safer user experiences across a wider range of online services.

3.13 In the March 2026 Consultation, we said, "we do not consider these proposals would have significant additional impacts on users or providers beyond those set out in the December 2024 Statement and the April 2025 Statement" This was not intended to suggest that the proposals have no impact on user safety. Rather, this statement reflects Ofcom's impact assessment, including assessing the impact of our proposed measures on users' rights.

3.14 Updates to the Register of Risks and Risk Profiles amount to "significant changes" to the Risk Profiles, meaning providers need to take appropriate steps to keep their Illegal Content Risk Assessments up to date. They would need to assess the risks of harm for suicide and self-harm and cyberflashing and assign appropriate risk levels to these harms. These changes are expected to improve services' understanding of how these harms may manifest

---

[26] Centre for Protecting Women Online response to March 2026 Consultation, pp.2-3; Molly Rose Foundation response to March 2026 Consultation, p.1; Online Safety Act Network (OSAN) response to March 2026 Consultation, p.3; Samaritans response to March 2026 Consultation, p.3.
[27] Molly Rose Foundation response to March 2026 Consultation, p.1; Samaritans response to March 2026 Consultation, pp. 3-4.
[28] End Violence Against Women Coalition (EVAW) response to March 2026 Consultation, p.4.
[29] End Violence Against Women Coalition response to March 2026 Consultation, p.3, South West Grid for Learning, response to March 2026 Consultation, p.3.
[30] Centre for Protecting Women Online response to March 2026 Consultation, p.4.
[31] The Online Safety Act 2003 (Priority Offences) (Amendment) Regulations 2025 amends the list of priority offences in Schedule 7 of the Act.

on their platforms and the risk they pose to users. In turn, this should enable providers to take more effective and proportionate steps to mitigate those risks.

3.15 The changes we are making to the Codes of Practice will ensure that relevant measures apply more consistently across services in relation to these harms. More services will be expected to:

a) provide users with tools to block and mute other users and to disable comments
b) carry out on-platform testing of recommender systems; and
c) allow users to easily report predictive search suggestions relating to suicide and self-harm and cyberflashing content and take appropriate steps to ensure reported suggestions are not recommended to any users.

3.16 Other measures, including those relating to governance and accountability, content and search and search moderation and user reporting and complaints, will also apply to a broader set of services as a result of these changes.

3.17 These changes may result in some additional costs and operational impacts for service providers. However, as set out in our consultation, we expect these impacts to be limited. This reflects the fact that our approach largely builds on existing processes and systems that many providers already have in place. This is not to mean that the proposed changes will not have a significant impact on users' safety.

3.18 We have not consulted on new Codes measures associated with these new priority offences at this stage, as we have prioritised ensuring that the framework reflects the new priority offences as quickly as possible, to ensure that users can benefit from the changes we have made. We expect to update our regulatory documents and guidance to respond to further legislative changes, technological developments and new evidence of illegal content.

Combining suicide and self-harm as one single kind of illegal harm

Our proposals

3.19 We proposed to combine the offence of encouraging or assisting suicide and the encouraging or assisting serious self-harm offence into a single kind of illegal harm, 'suicide and self-harm'.

Stakeholder feedback

3.20 Several service providers said they agreed with combining the two offences. They noted that it will result in a clearer, more effective and comprehensive risk assessment process, and consistency in the deployment of mitigations.[32] Others argued Ofcom should consider further consolidation of overlapping harms to improve the efficiency of the implementation of the Act.[33] Many civil society stakeholders and one academic stakeholder also expressed general agreement to combine the two offences as a single kind of illegal harm, noting they agree the harms manifest similarly and overlap in risk factors.[34]

[32] Microsoft response to March 2026 Consultation, p.1; Middle Tech Coalition response to March 2026 consultation, p. 2; LinkedIn response to March 2026 Consultation, p. 2.
[33] Middle Tech Coalition response to March 2026 Consultation, p. 2.
[34] National Confidential Inquiry into Suicide and Safety in Mental Health response to March 2026 consultation, p.1; Online Safety Act Network response to March 2026 Consultation, p.1; Samaritans response to March 2026 Consultation, p.1; [✂], p. 1; Centre for Protecting Women Online response to March 2026 Consultation, p. 3; Molly Rose Foundation response to March 2026 Consultation, pp. 2-3.

Clear guidance needed on differences and nuance of suicide and self-harm content

3.21 Some civil society organisations warned that combining suicide and self-harm could risk obscuring important differences in how these harms manifest.[35] A number of civil society organisations explained how the harms differed in intent, context, and identification, and highlighted the importance of providing distinct definitions, clearer guidance, and tailored approaches even if combined.[36]

3.22 Cetatea Viitorului said suicide and self-harm differed in intent, vulnerability patterns, and interventions. It recommended keeping a single category but using separate detection models and intervention protocols for suicide and self-harm content.[37] South West Grid for Learning said self-harm content was more complex to define, detect, and moderate compared to suicide content.[38]

3.23 Internet Matters said it is important to maintain sufficient nuance in how these harms are understood, especially for children, due to ambiguity in self-harm content. It cited guidance from Samaritans on the difficulty of distinguishing harmful and supportive content and reported its own research showing that 6% of children aged 13–17 had encountered such content. It recommended clear guidance to preserve distinctions and support services.[39]

3.24 Centre for Protecting Women Online warned that combining the two offences could obscure important differences, noting evidence from YoungMinds and Refuge that self-harm content affecting girls and young women was often normalised within peer groups, unlike suicide-related content which was more linked to immediate crises. It added that these harms were shaped by inequalities, with certain groups including girls and young women, especially those who identify as LGBTQ+, disabled or from minoritised backgrounds, more likely to experience self-harm and other types of abuse online. It argued services should assess risk in a gender- and context-sensitive way.[40]

3.25 Online Safety Act Network said both harms were difficult to define and identify, especially self-harm content. It said Ofcom should identify which services are likely to have a significant risk of incidence of suicide and self-harm material. It explained that suicide content was most dangerous when instructional and often found in small forums, while harmful self-harm content could involve bullying or abuse in private or small groups. It said any combined approach must clearly explain these differences to service providers.[41]

3.26 Samaritans, Online Safety Act Network, and South West Grid for Learning noted the nuance around self-harm content specifically, arguing certain types of this content should not be treated as encouragement of self-harm, for example harm reduction, minimisation, or

---

[35] Cetatea Viitrorului response to March 2026 Consultation, p. 2; Internet Matters response to March 2026 Consultation, p.1; Centre for Protecting Women Online response to March 2026 Consultation, p. 3; Online Safety Act Network response to March 2026 Consultation, p.1; South West Grid for Learning response to March 2026 Consultation, p. 1; Molly Rose Foundation response to March 2026 Consultation, p. 3.
[36] Cetatea Viitrorului response to March 2026 Consultation, p. 2; Internet Matters response to March 2026 Consultation, p.1; Centre for Protecting Women Online response to March 2026 Consultation, p. 3; Online Safety Act Network response to March 2026 Consultation, p.1; South West Grid for Learning response to March 2026 Consultation, p. 1; Molly Rose Foundation response to March 2026 Consultation, p. 3; Samaritans response to March 2026 Consultation, p.1.
[37] Cetatea Viitrorului response to March 2026 Consultation, p. 2.
[38] South West Grid for Learning response to March 2026 Consultation, p. 1.
[39] Internet Matters response to March 2026 Consultation, p.1.
[40] Centre for Protecting Women Online response to March 2026 Consultation, p. 3
[41] Online Safety Act Network response to March 2026 Consultation, pp.1-2

recovery content, content relating to personal stories of self-harm, or artistic depictions of self-harm content. [42] Some noted unclear guidance could lead to the over-removal of this type of content.[43] South West Grid for Learning said services needed clear guidance on what constitutes encouragement or assistance,[44] and Molly Rose Foundation said services generally needed clearer guidance on what illegal self-harm content is.[45]

Multi-risk measures and scope

3.27 Samaritans and the Online Safety Act Network also noted that combining the suicide and self-harm offences will mean that smaller services both at risk of suicide and self-harm and no other illegal harms, that would otherwise have been multi-risk and therefore in scope of measures which apply to multi-risk services, will now not be in scope of these measures.[46] Samaritans asked Ofcom to clarify how this has been considered and the impact this has on tackling harms on smaller platforms.[47]

Our decision

3.28 We have decided to confirm our proposal to combine the offences of encouraging or assisting suicide and encouraging or assisting serious self-harm into a single kind of illegal harm. This means that providers will need to assess the risk of both harms and assign an overall risk level to 'suicide and self-harm'. It also means that relevant Codes measures that specifically apply to suicide content or services at medium or high risk of suicide should also apply to self-harm content and relevant services at medium or high risk of self-harm.[48] Finally, it means that measures we proposed as part of our June 2025 Consultation which apply to user-to-user services with relevant characteristics at medium or high risk of illegal suicide (if made and in whichever form they take), should also apply to illegal self-harm content and relevant services at medium or high risk of illegal self-harm.[49]

Difference in how the harms manifest, and a need for clear guidance

3.29 We recognise that suicide and self-harm content can manifest in different ways and that it is important to ensure that service providers recognise this. We already provide guidance across our Illegal Harms and Protection of Children products to reflect differences in how suicide and self-harm content manifests. For example, when evidence is only relevant to one or the other harm, we make this clear in our Register of Risks. We have also chosen to keep the guidance on the two offences separate in the Illegal Content Judgement Guidance to ensure services consider how content that amounts to these offences differ from each other.

---

[42] Samaritans response to March 2026 Consultation, p.1; Online Safety Act Network response to March 2026 Consultation, p.1; South West Grid for Learning] response to March 2026 Consultation, p. 2.
[43] Samaritans response to March 2026 Consultation, p.1; Online Safety Act Network response to March 2026 Consultation, p.1; [✂]
[44] South West Grid for Learning] response to March 2026 Consultation, p. 2.
[45] Molly Rose Foundation response to March 2026 Consultation, p. 3.
[46] Samaritans response to March 2026 Consultation, p.1; Online Safety Act Network response to March 2026 Consultation, p.1.
[47] Samaritans response to March 2026 Consultation, p.1.
[48] This includes: On-platform testing of recommender systems (ICU E1); Reporting of predictive search suggestions (ICS F1); Provision of crisis prevention information (ICS F3); Blocking and muting (ICU J1); and Disabling comments (ICU J2).
[49] We will confirm our decisions in relation to the additional safety measures proposed in the June 2025 Consultation in Autumn 2026.

3.30 We expect services to reflect the differences in how these two harms manifest when they carry out their duties, for example by drawing on different evidence inputs, considering the varying impacts associated with each harm, and applying measures that capture and mitigate each harm.

3.31 In the relevant Register of Risks and Illegal Content Judgements Guidance chapters, we highlight the nuances of both suicide and self-harm content. In particular, we note that suicide and self-harm content is likely to be posted by people – including children – in vulnerable and difficult circumstances and may be posting this content to find supportive communities and express their own experiences. They may be intending to help others and may not have a full understanding of the harm which may arise from the content they are posting.[50]

3.32 In the Illegal Content Judgements Guidance we note that while this does not negate providers' duties, for example, to remove illegal content (for user-to-user services), or to minimise the risk of users encountering illegal content (for search services), providers should be aware that the over-removal of non-illegal content relating to suicide or self-harm may have a negative impact on the person posting, for example, by exacerbating feelings of isolation or self-criticism. We explain that over-removal may also contribute to the stigma around openly discussing mental health challenges, difficult life circumstances, suicidal thoughts, and experiences or thoughts of self-harm. We therefore ask services to be mindful of this when for instance making illegal content judgements about this type of content.[51]

3.33 Our Illegal Content Judgements Guidance provides clear and detailed guidance on what 'encouragement' or 'assistance' with 'intent' is, to further support service providers' illegal content judgements. We explain that in some cases where specific, practical or instructional content on self-harm methods is posted, it would not be reasonable to infer intent to encourage or assist serious self-harm. For example, when the intent behind posting method information can reasonably be inferred to be to promote harm minimisation or safety promotion (for example, promoting less dangerous ways to self-harm, or to counter another suggestion), or where the method is described in the context of personal experience (without being promoted for replication by others).

Multi-risk measures and scope

3.34 Our policy intent when we published our March 2026 Consultation was to align illegal self-harm content protections with current illegal suicide content protections. This is because much of the evidence relevant to suicide and self-harm risks online is the same or overlaps, demonstrating that suicide and self-harm have the same risk factors. We have concluded that the most proportionate way to align self-harm with suicide is to combine the two offences.

3.35 We remain of the view, as set out in our Consultation, that the measures that apply to services to protect people from encountering illegal suicide content will also be effective in protecting people from encountering illegal self-harm content.[52] For example, evidence demonstrates that the ability to comment on content increases the risk of users

[50] Ofcom, 2024. Illegal Content Judgements Guidance, p. 177; Ofcom, 2024. Illegal Harm Register of Risks, p. 312.
[51] Ofcom, 2024. Illegal Content Judgements Guidance, p. 177.
[52] Ofcom (2026), Consultation Illegal Harms Updates for New Priority Offences, pp. 17-36.

encountering self-harm content.[53] We therefore noted in our Consultation that by recommending that large services at medium or high risk of suicide and self-harm implement the disabling comments measure,[54] this will reduce the risk of users encountering these specific kinds of illegal content.[55] Similarly, in our March 2026 Consultation we said that providing self-harm crisis prevention information when users search for content relating to self-harm or instructions for self-harm methods would provide the same benefits for users as those discussed in relation to suicide, namely how this can disrupt a search journey that might otherwise have led them to encounter illegal content amounting to the offence of encouraging or assisting serious self-harm.[56]

3.36 An alternative approach would have been to treat self-harm as a separate, standalone harm category. As raised by Samaritans and the Online Safety Act Network, doing so could have resulted in some services – those only at risk of suicide and self-harm – being brought within scope of a number of other measures that apply to multi-risk, but not single-risk, services.[57] Our analysis suggest that there are not many services that are only at risk of suicide and self-harm. We consider that there would only be marginal benefits associated with a small number of services that are only at risk of self-harm and suicide separately coming in scope of measures for multi-risk services, while incrementally increasing the cost and complexity of compliance for services more generally. As such, we have concluded that the protections that will apply under a combined framework will help to address the risks associated with serious self-harm in the most proportionate way.

3.37 We are confident that we can take appropriate enforcement action where we have concerns that risks are not being effectively mitigated by services, regardless of whether they are single-risk or multi-risk. We have recently issued a confirmation decision in relation to a suicide discussion forum.[58]

Generative AI

Stakeholder feedback

3.38 The National Confidential Inquiry into Suicide and Safety in Mental Health agreed with our changes to the Register to reflect up-to-date evidence including research on AI chatbots.[59] Samaritans said it was pleased that the Register now includes research on AI chatbots, which it said highlights potential risks from some generative AI systems that may produce harmful self-harm or suicide-related outputs.[60]

---

[53] Ofcom (2024), Register of Risks p. 366.
[54] ICU J2.
[55] Ofcom (2026), Consultation Illegal Harms Updates for New Priority Offences, p. 28
[56] Ofcom (2026), Consultation Illegal Harms Updates for New Priority Offences, p. 33.
[57] For example, the following measures in the User-to-User Code apply to large or multi-risk services: ICU A3 (Written statements of responsibilities); ICU A5 (Tracking evidence of new and increasing illegal harm); ICU A6 (Code of conduct regarding protection of users from illegal harm); ICU A7 (Compliance training); ICU C3 (Setting internal policies); ICU C4 (Performance targets); ICU C5 (Prioritisation); ICU C6 (Resourcing); ICU C7 (Provision of training and materials to individuals working in content moderation (non volunteers)); ICU C8 (Provision of materials to volunteers); ICU D8 (Appropriate action for relevant complaints which are appeals – determination (large or multi risk services)).
[58] **Content warning:** the linked webpage contains discussion of illegal suicide content which some people may find distressing. Investigation into an online suicide discussion forum and its compliance with duties to protect its users from illegal content [accessed 15 June 2026].
[59] National Confidential Inquiry into Suicide and Safety in Mental Health response to March 2026 Consultation, p.2.
[60] Samaritans response to March 2026 Consultation, p.2.

3.39 Online Safety Act Network and Samaritans called for clarity around when Ofcom will update the regulatory products to incorporate risks of generative AI, how it will build the evidence base to do this and why it has not made the updates to date.[61]

3.40 End Violence Against Women Coalition and Molly Rose Foundation called for Ofcom to include generative AI in the Risk Profiles.[62]

3.41 Internet Matters and End Violence Against Women Coalition called for Ofcom to urgently prioritise future work to incorporate AI-enabled risks into regulatory products.[63] Centre for Protecting Women Online highlighted that generative AI is increasing the level of harm to women and girls online.[64]

3.42 Centre for Protecting Women Online and Samaritans expressed concerns that some generative AI services may not currently be in scope of the Act.[65]

Our decision

3.43 We have decided to confirm the position we proposed in the March 2026 Consultation, which is to not include generative AI (GenAI) in the Register of Risks and Risk Profiles at this stage.

3.44 We remain of the view that appropriately capturing GenAI as a risk factor would require a more comprehensive update to the Register of Risks and Risk Profiles, considering multiple kinds of priority illegal harms, not only the two new priority offences. Doing this would have delayed our ability to consult on the changes needed to reflect the new priority offences.

3.45 We monitor how the use of AI is evolving across all illegal harms and we are continuing to build our evidence base exploring the changing ways people are using AI and the online safety that risks that may emerge and what it means for our Register of Risk and Risk Profiles.[66]

3.46 Our Codes measures already apply to GenAI content where it is shared by users on user-to-user services, and to GenAI services where they fall within the scope of the Act. [67] Providers should therefore take swift and appropriate action in respect of AI-generated content that is illegal or harmful to children.

3.47 Finally, we are closely monitoring proposed legislative changes relating to GenAI, including through the Crime and Policing Act, and are working closely with government to understand the policy work that may be needed to implement the additional protections it is will bring for users.

---

[61] Online Safety Act Network response to March 2026 Consultation, p.8; Samaritans response to March 2026 Consultation, p.2.
[62] End Violence Against Women and Girls Coalition response to March 2026 Consultation, p.2; Molly Rose Foundation response to March 2026 Consultation, p.4.
[63] Internet Matters response to March 2026 Consultation, p.2; End Violence Against Women and Girls Coalition response to March 2026 Consultation, p.2.
[64] Centre for Protecting Women Online response(s) to March 2026 Consultation, p.4.
[65] Centre for Protecting Women Online response to March 2026 Consultation, P.3.; Samaritans response to March 2026 Consultation, p.2.
[66] Ofcom, 2025. AI chatbots and online regulation – what you need to know
[67] Ofcom 2024 Open letter to UK online service providers regarding Generative AI and chatbots

Com groups

Our proposals

3.48 We proposed to add evidence to our Register of Risks which explains how Com groups[68] often utilise direct and group messaging functionalities to groom and manipulate victims, including encouraging self-harm.

Stakeholder feedback

3.49 Molly Rose Foundation expressed concern about the lack of specific measures addressing Com groups, despite their inclusion in Ofcom's updated Register of Risks and Risk Profiles, arguing that no measures addressed key harm pathways such as messaging or livestreaming despite growing evidence of risk. It said this reflected poor regulatory strategy.[69]

3.50 It referenced its own evidence and evidence from the NCA to argue that, as Com groups use grooming techniques across multiple crimes, Ofcom should adopt a more integrated approach linking grooming with suicide and self-harm offences.[70]

Our decision

3.51 We have decided to confirm the position we proposed in the March 2026 Consultation and not to develop specific measures for Com groups at this time.

3.52 We share Molly Rose Foundation's concerns relating to Com groups. In response to concerns from organisations such as Molly Rose Foundation and a growing evidence base about the expansion of these groups, we proposed in our March 2026 Consultation to add evidence to our Register of Risks which explains how Com groups often utilise specific functionalities, such as direct and group messaging, to groom and manipulate victims, including encouraging self-harm.[71] Based on changes proposed at consultation, we are now including direct and group messaging in the Illegal Harms User-to-User Risk Profile. This means that, when doing their Risk Assessment, providers of services with these functionalities will need to assess whether those functionalities increase the risk of illegal content relating to suicide and self-harm being present or disseminated on the service, or whether the service could be used to commit or facilitate these priority offences. This may include where offences are being perpetrated by Com group members.

3.53 Our March 2026 Consultation focused on aligning self-harm and cyberflashing with other priority illegal harms. As such, we would not at this stage develop new Codes measures. We expect to update our regulatory documents and guidance again in due course to respond to further legislative changes, technological developments and new evidence on illegal content. The majority of the measures in our Illegal Harms and Protection of Children Codes are harms agnostic and apply across all illegal harms or content harmful to children. We are confident that many risks posed by Com groups will already be addressed by these existing

---

[68] The National Crime Agency, 2025, referred to 'Com groups' as "online networks of individuals who carry out serious, high-harm offences including child sexual abuse, serious violence, cybercrime (referred to as cyber Com), and extremism. Com groups are dynamic and often overlap across these threats, although not every case will involve all. Within these groups, offenders may compete against one another to cause the highest harm to gain status and notoriety. Offenders may do so by creating and sharing harmful and extreme content, for example, child sexual abuse material (CSAM), or by coercing victims, often under 18-year-olds, to commit harmful acts towards themselves or others, such as inflicting injuries."

[69] Molly Rose Foundation response to March 2026 Consultation, pp.2 and 5

[70] Molly Rose Foundation response to March 2026 Consultation, p.3

[71] Register of Risks 'Suicide and self-harm', paragraph 15.86 and 15.87 on Direct Messaging and Group Messaging.

measures. In addition, some of our June 2025 Consultation's proposed additional measures are intended to add further protection to users where livestreams containing suicide or self-harm content carry the risk of imminent physical harm. We will publish our decisions in relation to this and other measures in autumn 2026.

3.54 Using the levers we already have, we are engaging with a targeted selection of medium to large services where Com Group activity is most prevalent, as well as a number of small but risky services, to assess what more they can do individually and collectively to prevent and/or detect harms arising from this activity. Ofcom's 'Small But Risky Taskforce' continues to work extensively with relevant services, including video sharing platforms dedicated to graphic violent content ("gore"), suicide and self-harm forums, and sites with a high risk of CSAM and grooming, using a variety of levers to reduce harms through deployment of highly effective age assurance or resulting in services geoblocking the UK. We also partner with law enforcement and child protection organisations to better understand the ecosystem and how these networks operate and adapt across platforms.

Repeat engagement and pattern level detection

Stakeholder feedback

3.55 Iris Anticipa said Ofcom's Risk Profiles, Register of Risks and Illegal Content Judgement Guidance should emphasise how repeat engagement, often taking place using messaging functions, is central to how the serious self-harm and cyberflashing offences are committed online. It argued that behavioural pattern detection can help identify this type of content.[72]

Our decision

3.56 We have decided to confirm our position from the March 2026 Consultation and will not update the Register of Risks, Risk Profiles or ICJG to include repeat engagement as a risk factor or make any other changes to our guidance to this effect. Our Illegal Harms User-to-User Risk Profiles include direct messaging and group messaging as risk factors for suicide and self-harm. It also includes direct messaging and messaging services as risk factors for cyberflashing. Accordingly, providers offering these functionalities must assess, as part of their risk assessments, whether they increase the risk of these offences occurring on their services. This includes the risks arising from cumulative or repeated interactions, as well as individual incidents. In the Register of Risks, we also recognise that in the case of cyberflashing, it can form part of a pattern of harm behaviour with some individuals reporting receiving several unsolicited images a day.

3.57 In the ICJG we say that where providers have other information not specified in the guidance, which is relevant to a content judgement, they may and should consider it. Therefore, where providers have relevant cumulative and pattern-level evidence, they should use this when making judgements about illegal self-harm or cyberflashing content.

3.58 We welcome the suggestion that pattern level detection would be effective in detecting repeat engagement, however, we are not proposing any new Codes measures in association with these new offences at this time. Please see paragraph 3.18 for further information.

[72] Iris Anticipa response to March 2026 Consultation, p.2.

Risk Assessment Guidance and Risk Profiles: general approach

Our proposals

3.59 To reflect the fact that the self-harm and cyberflashing offences have been designated as 'priority offences' by the government, we proposed to update the lists of kinds of illegal harm which providers need to assess separately. We proposed to combine the self-harm offence with encouraging or assisting suicide into a single kind of illegal harm, 'suicide and self-harm'. We proposed to include cyberflashing as a new kind of illegal harm that providers should separately risk assess for in their risk assessments. We did not propose to make any substantive changes to the Risk Assessment Guidance.

3.60 We proposed to update the User-to-User Risk Profile to include the risk factors associated most strongly with cyberflashing and encouraging or assisting serious self-harm. We also proposed to add a reference to self-harm to the Search Risk Profile. We provisionally considered these proposals amounted to a significant change to the Risk Profile meaning providers would need to update their risk assessments.

Stakeholder feedback and our decision

3.61 End Violence Against Women Coalition agreed that service providers should risk assess for cyberflashing[73] and Internet Matters agreed with the proposed risk factors for cyberflashing.[74] Samaritans and OSAN both supported the addition of new risk factors for suicide and self-harm in the Risk Profiles.[75]

3.62 We have decided to confirm these decisions.

Risk Profiles

Stakeholder feedback and our decision

Significant change to Search Risk Profile

Our proposals

3.63 We proposed to update the Risk Profiles. We provisionally considered that this would amount to a significant change to the Risk Profiles, meaning that providers would need to update their risk assessments.

Stakeholder feedback

3.64 Middle Tech Coalition suggested that adding the additional reference to 'self-harm' in the Search Risk Profile does not constitute a 'significant change' to the risk profile for providers of low-risk services without relevant functionalities. It suggested that we should define 'significant change' to clarify when risk assessments must be update.[76]

Our decision

3.65 We have decided to confirm our proposal that the changes we are making constitute a significant change to the Risk Profiles.

---

[73] End Violence Against Women Coalition (EVAW) response to March 2026 Consultation, p.1.
[74] Internet Matters response to March 2026 Consultation, p.2.
[75] OSAN Online Safety Act Network and Samaritans responses to the March Consultation, Q2.
[76] Middle Tech Coalition response to March 2026 consultation, p. 3.

3.66 Providers are required to take account of the relevant Risk Profile when conducting their risk assessment. The updated Risk Profiles identifies risk factors that are associated with the new kinds of illegal harm and will therefore need to be reflected in the risk assessment. As such, it is not an immaterial amendment. Taken together, the changes set out in this statement (including the addition of 'self-harm' to the Search Risk Profile) amount to a "significant change" to both User-to-User and Search Risk Profiles.

3.67 Under the Act, providers must take appropriate steps to keep a risk assessment up to date, including when Ofcom make any significant change to a risk profile. Paragraphs 2.50 -2.53 of the Risk Assessment Guidance provides further information.

Additional risk factors for cyberflashing

Our proposals

3.68 We proposed that our Illegal Harms User-to-User Risk Profile listed cyberflashing as a risk factor for social media services, messaging services, user profiles, anonymous user profiles, user connections, direct messaging and posting images or videos. This means that when doing their Risk Assessment, services with these characteristics or functionalities will need to consider the risks of harm from cyberflashing.

Stakeholder feedback

3.69 End Violence Against Women Coalition argued that dating services should be specified as a risk factor a, noting that the Register of Risks acknowledges that cyberflashing is particularly prevalent on these services.[77] Relatedly End Violence Against Women Coalition expressed surprise that Ofcom did not think the extension of certain existing Codes measures to cyberflashing would bring additional services into scope, noting that dating services are high risk for cyberflashing.[78]

3.70 Some stakeholders also suggested the cyberflashing Risk Profile should better reflect overlaps with other harm areas. End Violence Against Women Coalition and Online Safety Act Network proposed cross-references to the extreme pornography and intimate image abuse Risk Profiles by adding discussion forums and chat rooms and reposting and forwarding content as risk factors for cyberflashing.[79]

3.71 LinkedIn argued that cyberflashing should be addressed within the harassment, stalking, threats and abuse harm area.[80]

Our decision

3.72 We have designed the Risk Profiles to be as effective as possible, extracting the most important findings from the Register of Risks in a way that is practical, simple and easy to follow by thousands of potentially regulated service providers encompassing a broad spectrum of service types and sizes. They are not intended to be an exhaustive list of all risks or service types identified in the Register of Risks but contain risk factors we consider particularly important for service providers to consider, based on our current evidence base. Service providers are required to take account of specific risk factors in their risk assessments.

---

[77] End Violence Against Women Coalition (EVAW) response to March 2026 Consultation, pp.1-2; Online Safety Act Network response to March 2026 Consultation, p.7.
[78] End Violence Against Women Coalition (EVAW), response to March 2026 Consultation, p.4.
[79] End Violence Against Women Coalition (EVAW) response to March 2026 Consultation, pp.2-4; Online Safety Act Network response to March 2026 Consultation, p.2 and p.5.
[80] LinkedIn response to our March 2026 Consultation, p.6.

3.73 The Risk Profiles do not include dating services as a specific service type risk factor for any category of harm, and we have decided to retain this approach following consultation. However, the risk factors for cyberflashing include user profiles, user connections and direct messaging – all of which appear extensively on dating services. We therefore consider that the risks of dating sites are already captured in the Risk Profiles.

3.74 We also expect service providers to consult the Register of Risks to assist them in identifying any specific characteristics that are not covered by the Risk Profiles and could increase the risk of harm. We set out in the Register of Risks that cyberflashing is particularly prevalent on dating services. Service providers are required to consider both the intended and unintended ways that people may use their service when conducting their risk assessments.

3.75 In the Register of Risks, we recognise that cyberflashing often occurs in conjunction with other online harms, including intimate image abuse and extreme pornography. However, the risk factors for all these harms are not necessarily the same. Our current evidence base does not suggest that discussion forums, chat rooms, or reposting and forwarding content increase the risks of harm in relation to cyberflashing.

3.76 Finally, in response to LinkedIn's point, we recognise that cyberflashing can occur in conjunction with cyberstalking and harassment. However, there are differences in how the harms manifest and the functionalities that increase the risk of the harm, so we have decided to confirm our proposal to add cyberflashing as a separate harm category.

Register of Risks

3.77 We proposed to make minimal changes to the Register of Risks. We proposed to add a small amount of new evidence relating to self-harm and cyberflashing that has been published since our first Illegal Harms Statement in December 2024.

3.78 Additionally, we proposed to remove terms of phrases relating to suicide or self-harm content which could potentially risk exposing users to harmful or illegal content.

Stakeholder feedback and our decision

Cyberflashing

Our proposals

3.79 We proposed to add limited new evidence related to cyberflashing to the Register of Risks, including updating evidence where relevant and recognising messaging services as a risk factor for cyberflashing.

Stakeholder feedback

3.80 Centre for Protecting Women Online stressed that cyberflashing should be clearly recognised as a form of sexual violence[81] and South West Grid for Learning shared that their frontline services consistently show that cyberflashing is targeted at women and is often used as a form of harassment, intimidation or sexualised abuse.[82] Online Safety Act Network provided additional evidence on cyberflashing.[83]

[81] Centre for Protecting Women Online response to March 2026 Consultation, p.4.
[82] South West Grid for Learning response to March 2026 Consultation, p.3.
[83] Online Safety Act Network response to March 2026 Consultation, Q5.

3.81 End Violence Against Women Coalition expressed concern that the evidence base cited for cyberflashing did not reflect the recent exponential increase in forms of image-based sexual abuse and reflected a minimal approach from Ofcom.[84]

3.82 End Violence Against Women Coalition also stressed that there is currently insufficient data on cyberflashing. They sought to understand how Ofcom will be developing and maintaining knowledge on cyberflashing, especially what mechanisms are in place for information sharing between Ofcom, the police and the Crown Prosecution Service.[85]

Our decision

3.83 The changes we proposed adding to the Register of Risks reflect the limited amount of evidence related to cyberflashing since December 2024. Where relevant evidence meeting our quality assurance criteria has been provided by stakeholders, we have incorporated it into the Register of Risks.[86] We have included the evidence provided by Online Safety Act Network demonstrating the disproportionate impact of cyberflashing on women.

3.84 In the Register of Risks, we recognise that there is limited research and evidence available on cyberflashing. We will update our Register of Risks over time as new risks, harms and evidence emerge. In doing so, we will continue to draw on a range of evidence including from academic institutions, civil society organisations and law enforcement.

Suicide and Self-harm

Our proposals

3.85 We proposed updating the suicide and self-harm chapter to include additional evidence on how these harms manifest online, including research on AI chatbots highlighting the risks of harmful suicide or self-harm related outputs, as well as potentially distressing responses for users seeking informal mental health support. We also included further evidence on messaging functionalities, showing how direct and group messaging could be used to pressure or encourage vulnerable users into self-harm or suicide.

Stakeholder feedback

3.86 Several civil society stakeholders agreed with the additional evidence that we proposed to add to the Register of Risks, particularly that which related to Com groups and group/direct messaging,[87] the competitive aspect of self-harm,[88] and eating disorders.[89]

3.87 Several stakeholders suggested other additional evidence to the Register of Risks, relating to recommender systems,[90] AI chatbots,[91] user connections,[92] user demographics,[93] and discussion forums.[94]

---

[84] End Violence Against Women Coalition (EVAW) response to March 2026 Consultation, pp.1-2.
[85] End Violence Against Women Coalition (EVAW) response to March 2026 Consultation, pp.2-3.
[86] We use a quality assurance process to ensure that all evidence contained within the Register of Risks meets high standards for method, ethics, reliability, independence and narrative.
[87] Molly Rose Foundation response to March 2026 Consultation, p. 3.
[88] Online Safety Act Network response to March 2026 Consultation, p.2.
[89] Online Safety Act Network response to March 2026 Consultation, p.2; Samaritans response to March 2026 Consultation, p.2.
[90] Centre for Protecting Women Online response to March 2026 Consultation, p. 3.
[91] Centre for Protecting Women Online response to March 2026 Consultation, pp. 3-4.
[92] Molly Rose Foundation response to March 2026 Consultation, p. 3; Resolver Trust and Safety, in partnership with Molly Rose Foundation (2025) Weaponised loneliness: Critical Harm Intelligence Briefing.
[93] Centre for Protecting Women response to March 2026 Consultation, p. 3.
[94] Molly Rose Foundation response to March 2026 Consultation, p. 4.

Our decision

3.88 Where relevant evidence meeting our quality assurance criteria has been provided by stakeholders, we have incorporated it into the Register of Risks.[95]

3.89 We have decided to add evidence on the following topics to our Register of Risks chapter on suicide and self-harm:

- AI chatbots
- User demographics
- Recommender systems
- Cyberbullying and self-harm link

Harm to children

Stakeholder feedback

3.90 South West Grid for Learning said that children are disproportionately exposed to self-harm content and peer-to-peer dynamics that may unintentionally normalise or reinforce harmful behaviours. It therefore urged Ofcom to ensure that child specific risk factors are explicitly referenced in Risk Profiles, that Codes of Practice clearly address how services should respond to self-harm content involving children, and that the involvement of a child within a report of self-harm content should be prioritised.[96]

Our decision

3.91 We discuss the risk of harm to different userbase demographics in the Register of Risks. This includes evidence on the impact on children more specifically, for example, that younger people are more likely to see or experience suicide or self-harm content.[97]

3.92 The Act provides an additional layer of protection for children from online harms. As such, our Children's Register of Risks addresses risk factors for children in more detail, including some that are specific to self-harm.[98] While the Children's Register of Risks considers content harmful to children rather than illegal content, some of the underlying evidence and risk factors are the same. Similarly, our Protection of Children Codes include measures services can implement to specifically prevent children from encountering content that is harmful to them, which includes content that promotes, encourages or provides instructions for self-harm.

Removing examples of terms or phrases relating to suicide or self-harm content

Our proposals

3.93 We included examples in the Register of Risks and Illegal Content Judgements Guidance of terms, phrases, euphemistic, and coded language relating to suicide and self-harm content when we published it as part of the 2024 Illegal Harms Statement. In our March 2026 Consultation, we proposed to remove these examples. We explained that we now consider that the inclusion of these examples could potentially draw attention to and risk exposing users to harmful or illegal content.

---

[95] We use a quality assurance process to ensure that all evidence contained within the Register of Risks meets high standards for method, ethics, reliability, independence and narrative.
[96] South West Grid for London response to March 2026 Consultation, p. 2.
[97] Ofcom, 2026. Register of Risks, pp. 306
[98] Ofcom 2025, Statement: Protecting children from harms online

Stakeholder feedback

3.94 Several stakeholders agreed with our proposals to remove such terms.[99] However, the National Confidential Inquiry into Suicide and Safety in Mental Health said that the issue was complex and highlighted that allowing services to access examples of known dangerous queries safely would enable more comprehensive safety solutions, despite evidence showing public dissemination of specific suicide-related details carries a tangible risk of harm.[100]

Our decision

3.95 We have decided not to include examples of terms, phrases, euphemistic or coded language relating to suicide and self-harm content in relevant regulatory products. Although it may be helpful for services to be aware of such examples, they will likely continue to change as services become more aware of this language, which may result in users changing the language they use to continue evading moderation. Therefore, including these terms for better identification in our products could become quickly outdated. Although we recognise that sharing such examples in a safe way could be beneficial for service providers, we do not think our public facing regulatory products is an appropriate place to do so. To conclude, we consider that the potential harm from vulnerable users engaging with these terms is a greater risk than the potential benefits of including the examples.

Illegal Content Judgements Guidance

3.96 We proposed structural changes to the Illegal Content Judgements Guidance (ICJG) to reflect the new status of self-harm and cyberflashing. This included moving self-harm and cyberflashing sections to the relevant parts of the ICJG which discuss priority offences and combining the suicide and self-harm chapters.

3.97 We also proposed to include sub-sections which discuss the types of illegal content providers may need to consider for the purposes of their risk assessment, and where relevant, inchoate offences, to mirror the guidance on priority offences. We proposed to remove paragraphs including examples of euphemistic or coded language which users may use to attempt to circumvent content moderation systems when posting harmful suicide and self-harm content. Instead, we proposed to add more detail explaining tactics users may use to evade content moderation.

Stakeholder feedback and our decision

State of mind requirement for cyberflashing

Our proposals

3.98 In the ICJG we set out the state of mind requirement ('mens rea' in legal terminology) for cyberflashing is (a) intent to cause distress, alarm or humiliation, or (b) where the image is sent to obtain sexual gratification, recklessness as to whether distress, alarm or humiliation will be caused. We proposed that when making an illegal content judgement it would be reasonable for service providers to infer the required intent or recklessness in cases where a user sends a photograph or film of genitals, except when there is evidence of consent

[99] Online Safety Act Network response to March 2026 Consultation, p.2; Samaritans response to March 2026 Consultation, p.2.
[100] National Confidential Inquiry into Suicide and Safety response to March 2026 Consultation, p.3.

from the receiver or the content is posted on a service where sending and receiving intimate images without prior agreement is a commonly accepted part of the culture.

Stakeholder feedback

3.99 We received conflicting stakeholder feedback in response to this proposal.

3.100 The dating service Grindr argued that the evidence base suggests cyberflashing is a harm that mostly affects women and that the regulation is framed to protect women. Grindr added that this overlooks the community and cultural norms of Grindr, whose users are largely gay and bisexual men, where image exchange is a routine feature of interactions. Grindr therefore suggested that on their platform, it is not reasonable to assume the required intent or recklessness for cyberflashing applies to all unsolicited sexual images.[101]

3.101 Grindr argued that these differences should be factored into the Risk Profiles and risk assessment process.[102] Grindr noted that it already provided users with the ability to block other users but expressed concern about the application of existing content moderation Code measures to adult dating services, arguing this could have disproportionate impacts, particularly on LGBT+ people.[103]

3.102 Online Safety Act Network and End Violence Against Women Coalition argued that Ofcom had created an "exemption" for sites where cyberflashing is commonly accepted, which is contrary to the law.[104]

Our decision

3.103 The offence of cyberflashing is committed by the intentional sending of an image of genitals with the intent of causing alarm, distress or humiliation or, where the image is sent for the purpose of obtaining sexual gratification, recklessness as to whether alarm, distress or humiliation would be caused. [105]

3.104 We have not created an "exemption" for cyberflashing in certain contexts. Cyberflashing is committed when both conduct (the sending of an image) and mental elements of the offence (the sender's intention/recklessness) are present or satisfied.

3.105 The Register of Risks highlights that evidence suggests in some circumstances unsolicited sexual images may be generally received positively, such as on certain dating platforms. The mental element may not be present or satisfied on platforms where sending intimate images is generally received positively.

3.106 In the Register, we note that this can be the result of different relationship dynamics in same sex relationships compared to heterosexual ones, with evidence suggesting that cyberflashing is largely perpetuated by men against women. This is not to minimise the impact that unwanted and unsolicited sexual images can have on men.

3.107 The ICJG supports service providers to make illegal content judgements, in this case cyberflashing. To make this judgement service providers must assess whether the elements necessary for the commission of the offence, including the state of mind element, are present or satisfied. Given the challenges for service providers in assessing the intent of

---

[101] Grindr response to March 2026 Consultation, pp.1-3.
[102] Grindr response to March 2026 Consultation, pp.1-3.
[103] Grindr response to March 2026 Consultation, pp.4-5.
[104] Online Safety Act Network response to March 2026 Consultation, p.3.
[105] Section 66A of Sexual Offences Act 2003.

users' actions, we set out in the ICJG that when a photograph or film of genitals has been sent, the state of mind requirement can reasonably be inferred by service providers.

3.108 We also set out that it would not be reasonable to infer the state of mind of the sender in cases where there is evidence of consent from the receiver, or the content is posted on a service where it is a commonly accepted part of the culture to send and receive intimate images without prior agreement. In these circumstances, service providers should assess whether the content is illegal by seeking to reach a reasonable inference based on the information available to them and the circumstances they are aware of. All service providers must assess the risk of cyberflashing on their service and implement the relevant recommended Codes measures or equivalent safety measures. This includes reviewing and assessing suspected cyberflashing content, which may require making an illegal content judgement.

3.109 We agree that the normalisation of cyberflashing does not minimise the harm caused. We have amended the language used in the Register of Risks to avoid this implication.

Guidance provided on the self-harm offence

Stakeholder feedback

3.110 Samaritans and South West Grid for Learning said platforms needed guidance beyond legal definitions to distinguish context around self-harm content. [106] Online Safety Act Network said the legal definition of self-harm is too broad, and noted Ofcom's guidance on the offence includes encouragement to cumulative acts that result in self-harm which it argued will create challenges in identifying individual pieces of content.[107]

3.111 Samaritans and South West Grid for Learning said clearer definitions were needed for eating disorder content, with Online Safety Act Network saying it was unclear if the encouragement of eating disorders was included.[108]

3.112 Online Safety Act Network said the guidance does not specify the type of act causing harm, only that it reaches the threshold of grievous bodily harm (or serious injury in Scotland) and noted while some acts of self-harm are clearly defined, other acts may not be obvious to platforms. It noted consideration will also need to be given to deliberate acts of self-injury that may have a cultural, religious or sexual context.[109]

Our decision

3.113 In the ICJG we set out guidance on the legal definition of the self-harm offence to help service providers assess whether content is illegal. We have specified that serious self-harm means self-harm amounting to: (a) in England and Wales and Northern Ireland, grievous bodily harm within the meaning of the Offences Against the Person Act 1861; and (b) in Scotland, severe injury, and includes successive acts (including omissions) of self-harm which cumulatively reach that threshold.

3.114 We set out that self-harm may take a passive or active form. That is, it might result from a positive action or from inaction. Both types may meet the definition of 'serious self-harm' if they have the capacity to result in really serious harm and/or severe injury. Some types of

[106] Samaritans response to March 2026 Consultation, p.1; Online Safety Act Network response to March 2026 Consultation, p.1; South West Grid for Learning response to March 2026 Consultation, p. 2.
[107] Online Safety Act Network response to March 2026 Consultation, p.1.
[108] Samaritans response to March 2026 Consultation, p.1; Online Safety Act Network response to March 2026 Consultation, p.1; South West Grid for Learning response to March 2026 Consultation, p. 2.
[109] Online Safety Act Network response to March 2026 Consultation, p.1.

eating disorder content may therefore amount to illegal self-harm content, for example, content which constitutes encouragement of another person to starve themselves to the point of serious harm and/or severe injury may be illegal content, subject to there being reasonable grounds to infer intent on the part of the poster to encourage or assist serious self-harm of a person.[110] We have not included specific examples of acts of harm which could potentially reach the threshold of serious self-harm. This is because the legal definition is broad and we do not think it would be helpful to attempt to be more specific in our guidance of what might reach this threshold. Including such detail could also potentially draw attention to extremely harmful acts.

3.115 We set out in the ICJG that the Act does not require service providers to make illegal content judgements, so long as the application of that service provider's own terms and conditions is sufficient to secure compliance with the duties in the Act in other ways. For example, if the service provider's own terms and conditions of use prohibit content that is wider than the definition of self-harm illegal content under the Act, then the service provider would be considered to have fulfilled its legal duties regarding takedown so long as it applied these terms and conditions properly. In practice, this means that services may continue to operate with regard to terms and conditions which prohibit more self-harm content than is required under the Act. However, we encourage providers to consider carefully the impacts of their choices on users' opportunities to express themselves.[111] Samaritans provides further industry guidance on how to manage online suicide and self-harm content which also includes other definitions of self-harm.[112]

3.116 The Act also provides an additional layer of protection of children in that they should not just be protected from encountering illegal content, but also primary priority content which includes content that promotes, encourages or provides instructions for acts of deliberate self-injury and eating disorders.[113] Our Guidance on content harmful to children provides examples of content, or kinds of content, that we consider to be, or consider not to be, primary priority content that is harmful to children, including self-harm and eating disorder content.[114]

Record Keeping and Review Guidance

3.117 We proposed to make minor changes to the Record Keeping and Review Guidance, changing '17 kinds of priority illegal content' to '18 kinds of priority illegal content'.

Stakeholder feedback and our decision

Record keeping data requirements

Stakeholder feedback

3.118 Iris Anticipa suggested that the Record Keeping and Review Guidance should accommodate metadata-level and trajectory-level evidence records where service providers use pattern-level or behavioural-signal detection as part of proactive measures.[115]

---

[110] Ofcom, 2024. Illegal Content Judgements Guidance, p. 182.
[111] Ofcom, 2024. Illegal Content Judgements Guidance, p. 3.
[112] Samaritans. Industry guidelines for managing self-harm and suicide content [accessed 1 June, 2026].
[113] Online Safety Act 2023,Sections 12(3)(a) and 61.
[114] Guidance on content harmful to children.
[115] Iris Anticipa response to March 2026 Consultation, p.3.

3.119 Centre for Protecting Women Online said that to understand whether measures are working, service providers should be required to collect better data, broken down by gender, as well as data on ICJG exposure to harm and AI generated content.[116]

Our decision

3.120 The Record Keeping and Review Guidance is intended to support service providers in meeting their record-keeping duties under the Act, including steps for conducting risk assessments, maintaining clear records and reviewing compliance regularly.

3.121 Providers are expected to include in their risk assessment records a list of the evidence used to assess risks. The guidance does not prescribe the form this evidence should take, and it may include, where relevant, evidence derived from pattern-level detection of behavioural-signal detection. Providers are also required to regularly review their compliance with the relevant duties.

Codes

3.122 We proposed to bring cyberflashing and self-harm into alignment with the other kinds of illegal harms covered by the Act. We explained that the effect of this proposal was that:

- Measures that apply to services that are multi-risk, would now also apply to services that are multi-risk because they are medium or high risk for cyberflashing or suicide and self-harm (in addition to at least one other kind of illegal harm);
- Measures that apply to services that are medium or high risk for any kind of illegal harm would now also apply to services that are medium or high risk of cyberflashing or suicide and self-harm; and
- Measures that set out that providers should take action for all kinds of illegal harm would now also apply to cyberflashing and self-harm content.

3.123 As a result of the proposal to combine suicide and self-harm into a single kind of illegal harm, we proposed that the measures we currently recommend for and specifically apply to suicide content or services at risk of suicide would now apply to self-harm content and relevant services at risk of suicide and self-harm.[117]

3.124 We also proposed that the measure relating to blocking and muting (ICU J1) should also apply to relevant services at risk of cyberflashing.

3.125 We proposed to update Table C (user-to-user services) and Table A (search services) in the Codes to include suicide and self-harm, and cyberflashing, and amend references to the kinds of harm in measures where relevant.

[116] Centre for Protecting Women Online response to March 2026 Consultation, p.4.

[117] This includes measures relating to on-platform testing of recommender systems (ICU E1), reporting of predictive search suggestions (ICS F1), provision of crisis prevention information (ICS F3), blocking and muting (ICU J1) and disabling comments (ICU J2). It also includes measures proposed in the June 2025 Additional Safety Measures Consultation relating to reporting imminent harm in livestreams (ICU D17), availability of human moderatos for livestreams (ICU C16), proactive technology (ICU C11 and ICU C12) and recommender systems (ICU E2).

3.126 We have decided to confirm all the proposals set out above and discuss our response to Codes-related stakeholder feedback below. The effects of these decisions are as set out above.[118]

Stakeholder feedback and our decision

Approach to Codes

Stakeholder feedback

3.127 Several civil society stakeholders called for more proactive measures in Codes to prevent harm before it occurs.[119] Verifymy and Iris Anticipa both noted that proactive detection of illegal harms such as self-harm and cyberflashing is technically feasible.[120] Iris Anticipa suggest behavioural-pattern detection could be an effective way to tackle harms such as cyberflashing in future.[121]

3.128 Samaritans expressed concern that we were not proposing additional Codes measures in the consultation, warning that this will undermine the impact of the changes to the risk assessment guidance.[122]

3.129 South West Grid for Learning suggested that applying existing measures may be insufficient for harms like self-harm and that services require clearer expectations on how to evidence compliance, particularly in relation to service design and recommender algorithms.[123]

3.130 Cetatea Viitorului suggested that Codes should place greater emphasis on service design, interaction patters and features and functionalities. It recommended the Codes set clearer expectations for providers to use early-stage detection signal, preventative friction and real-time user support mechanisms. [124]

3.131 Molly Rose Foundation said Ofcom's failure to act left significant gaps in addressing the scale and evolving nature of online suicide and self-harm offences. It argued that these gaps would remain even if the measures proposed in the Additional Safety Measures consultation were introduced, referring to its response to this consultation.[125]

Our decision

3.132 We did not propose substantive updates to the Codes at this stage, recognising that the development and consultation of new measures is necessarily time intensive. Instead, we prioritised consulting quickly to ensure providers can respond to changes to the status of priority offences. We expect the changes confirmed in this document to have positive impacts on user safety from applying a consistent package of protections to the two new priority offences. The measures act on complementary parts of the risk chain: governance,

---

[118] Measures that already relate to all illegal content (including non-priority illegal content) are not affected by our decisions as they already apply to cyberflashing and self-harm content. Similarly, measures that apply to all services regardless of risk are not affected by our decisions. Measures that relate to other kinds of illegal harm specifically (for example, CSAM, grooming or fraud) are also unaffected.

[119] Molly Rose Foundation response to March 2026 Consultation, p.5; Online Safety Act Network response to March 2026 Consultation, p.4; Centre for Protecting Women Online response to March 2026 Consultation, p.2, 4; Cetatea Viitorului response to March 2026 Consultation, p.3.

[120] Verifymy response to March 2026 Consultation, p.3; Iris Anticipa response to March 2026 Consultation, p.3.

[121] Iris Anticipa response to March 2026 Consultation, p.3.

[122] Samaritans response to March 2026 Consultation, p.2.

[123] South West Grid for Learning response to March 2026 Consultation, p.3.

[124] Cetatea Viitorului response to March 2026 Consultation, p.1, 3.

[125] Molly Rose Foundation response to March Consultation, pp. 1-2.

detection and moderation, recommender systems and search, reporting and crisis support, and user controls. Taking these together should reduce the likelihood and duration of exposure to illegal self-harm and cyberflashing content.

3.133 We expect to update our regulatory documents and guidance again in due course to respond to further legislative changes, technological developments and new evidence of illegal content. As set out in our report Online Safety in 2025, if further Codes measures are required, we expect to consult on these in late 2027, with the new measures coming into force in late 2028.[126]

3.134 The Crime and Policing Act 2026 introduces a number of additional new offences and priority offences. We are currently scoping the additional policy work needed to respond to these new priority offences, with substantive policy development expected after the offences have been commenced by the government. As part of this wider programme of work, we are exploring whether it will be appropriate to consult on new Codes measures associated with the priority offences, including with those included in this statement.

Services in scope

Stakeholder feedback

3.135 Online Safety Act Network called for us to clarify whether additional services would be brought into scope of the Codes measures as a result of our proposals.[127]

Our decision

3.136 A small number of services could newly come into scope where inclusion of the new offences changes a service's Risk Profile e.g., becoming multi-risk, or where a measure applies because the service has the relevant characteristics.

Measures for services at risk of cyberflashing

Our proposals

3.137 We proposed to apply the measure relating to user blocking and muting (ICU J1) should also apply to relevant services at risk of cyberflashing.

Stakeholder feedback

3.138 Online Safety Act Network, End Violence Against Women Coalition and South West Grid for Learning supported our proposal to extend measures on user blocking and muting (ICU J1) to cyberflashing.[128]

3.139 End Violence Against Women Coalition also argued that more consideration is required in relation to recommender systems for cyberflashing, highlighting that algorithms can drive content relating to cyberflashing which in turn normalises this harmful behaviour.[129]

Our decision

3.140 Evidence demonstrates that user profiles and user communication functionalities increase the risk of users experiencing cyberflashing. We therefore decided to extend the user

---

[126] Ofcom, 2025. Online Safety in 2025: Summary of the technology sectors response to online safety rules

[127] Online Safety Act Network response to March 2026 Consultation, p.5.

[128] End Violence Against Women Coalition (EVAW) response to March 2026 Consultation, p.3; Online Safety Act Network response to March 2026 Consultation, pp.4-5; South West Grid for Learning response to March 2026 Consultation,p.3.

[129] End Violence Against Women Coalition (EVAW) response to March 2026 Consultation, pp.3-4.

blocking and muting measure (ICU J1) to relevant services at risk of cyberflashing to reduce the risk of cyberflashing on those services.

3.141 We are not aware of evidence suggesting that content recommender systems increase the risk of users experiencing cyberflashing. We therefore are not extending the testing of content recommender systems measure (ICU E1) to relevant services at risk of cyberflashing.

4. Next steps

4.1 Alongside this statement, we have published updated versions of the Risk Assessment Guidance and Risk Profiles, Illegal Harms Register of Risk, ICJG and Record Keeping and Review Guidance.

4.2 The amendments to the Codes will be implemented separately. We have published alongside this document draft consolidated versions of the relevant Codes incorporating the draft amendments that Ofcom intends to submit to the Secretary of State.

4.3 Their implementation will be subject to parliamentary process, and the amendments will come into force once this process is completed. We will provide updates on the timing of this process.

4.4 In the March 2026 Consultation, the draft updates to the Codes included amendments to the user control measures additional measures proposed in the April 2025 Illegal Harms Consultation on User Controls (April 2025 Consultation) and additional safety measures proposed in the June 2025 Additional Safety Measures Consultation (June 2025 Consultation). We have not yet reached final decisions on the majority of these proposals.[130] This statement therefore focuses solely on the changes proposed in the March 2026 Consultation.

4.5 We expect to publish our decisions on the amendments to the user control measures proposed in our April 2025 Consultation and the remaining additional safety measures proposed in our June 2025 Consultation in autumn 2026.

Keeping illegal content risk assessments up to date

4.6 The Act requires providers to assess the risks on their service associated with priority offences and other illegal content. It also requires them to review and revise their illegal content risk assessments to keep them up to date, including when Ofcom makes a significant change to a Risk Profile that relates to the service.[131] We consider that the changes set out in this statement amount to a "significant change" to both User-to-User and Search Risk Profiles.

4.7 Providers must review and update their illegal content risk assessments to assess the risks of the new kinds of illegal harm arising on their service. We recommend providers do this as soon as practical after publication.

4.8 Regarding the measures that services should consider to mitigate the risk of harm from these new priority offences, providers should consider the updated Codes as soon as they complete the parliamentary process and come into force.

[130] See footnote 23.
[131] Sections 9(3) and 26(3) of the Act.

A1. Legal framework

A1.1 In this annex, we set out the statutory basis of Ofcom's role and the issues we must consider when preparing Codes. As set out in the March 2026 Consultation and in this statement, we did not propose to make any substantive changes to the Codes. Instead, our proposals and decisions change how some of the measures apply.

The Online Safety Act 2023 and the Codes of Practice

A1.2 The Online Safety Act 2023 (the Act) is a set of laws designed to protect all UK users online, including children, by placing duties on a range of user-to-user and search service providers. The duties on service providers include identifying, mitigating and managing the risk of harm caused by illegal content and activity, including intimate image abuse.

A1.3 The Act establishes Ofcom as the regulator responsible for online safety. It places a requirement on us to prepare and issue Codes, which are a package of measures recommended for service providers to comply with their safety duties.

A1.4 The safety duties in the Act only apply to the design, operation and use of services in the United Kingdom (UK).[132] They also apply to the design, operation and use of a service as it affects UK users (i.e., duties that relate to users).[133] The Code measures must therefore relate to the design or operation of a service that operates in the UK and/or as it affects UK users of the service.[134]

A1.5 In December 2024[135] and April 2025,[136] we published our Illegal Content Codes of Practice and Protection of Children Codes of Practice, which set out a series of measures that aim to protect users online. Service providers should implement these measures to be compliant with their obligations in the Act. These Codes are a "safe harbour", as set out in the Act, which means that service providers who implement all applicable measures will be treated as compliant with their relevant duties under the Act.

A1.6 However, service providers are permitted, under the Act, to comply with their safety duties by implementing "alternative measures." In these cases, a service provider needs to retain a record of relevant decisions (i.e., the alternative measures) and explain how the relevant safety duties have been met. They are also expected to carefully consider the rights of users, including the right to freedom of expression and privacy.

A1.7 Under the Act, we are required to prepare and issue the following sets of Codes for user-to-user and search service providers (i.e., Part 3 services):

a) A Code covering terrorism content (relating to the offences set out in Schedule 5);
b) A Code covering child sexual exploitation and abuse content (relating to the offences set out in Schedule 6); and
c) One or more Codes for the purpose of compliance with other relevant duties (including but not limited to those relating to the offences set out in Schedule 7).

[132] This is defined in section 4 of the Act.
[133] Section 8(3) of the Act.
[134] Schedule 4 to the Act, paragraph 11.
[135] Ofcom, 2024. Statement: Protecting People from Illegal Harms Online.
[136] Ofcom, 2025. Statement: Protecting Children from Harms Online.

A1.8 We have issued four Codes that collectively meet this obligation: (1) the Illegal Content user-to-user Codes; (2) the Illegal Content search Codes; (3) the Protection of Children user-to-user Code; and (4) the Protection of Children search Code. Taken as a whole, the measures set out in these Codes address a range of illegal harms, for both adults and children, that are identified as priorities in the Act.

Ofcom's duties and online safety functions

A1.9 This section sets out the statutory basis of Ofcom's role and the issues we must consider when preparing Codes.

Ofcom's general duties under the Communications Act 2003

A1.10 Ofcom is the independent regulator for communications services. We have regulatory responsibilities for the telecommunications, post and broadcasting sectors, as well as for online services.

A1.11 As a public authority, Ofcom must act lawfully, rationally and fairly.

A1.12 The Communications Act 2003 (the 2003 Act) places duties on Ofcom that need to be fulfilled when exercising our regulatory functions, including for online safety. The 2003 Act sets out our principal duty is:

a) To further the interests of citizens in relation to communication matters; and
b) To further the interests of consumers in relevant markets, where appropriate by promoting competition.[137]

A1.13 In performing that principal duty, the 2003 Act sets out that Ofcom's regulatory activities need to be transparent, accountable, proportionate, consistent and targeted only at cases where action is needed.[138] We further need to ensure that UK citizens are properly protected from harm caused by content on regulated services. We achieve this by requiring service providers to use suitable systems and processes that help minimise the risk of harm.

A1.14 The 2003 Act further requires[139] that Ofcom must have regard to several factors, as they appear to us to be relevant in the circumstances,[140] and as a result we have carefully considered the following in making our decisions:

a) The risk of harm to UK citizens presented by regulated services;
b) The need for a higher level of protection for children than for adults;
c) The need for it to be clear to providers of regulated services how they may comply with their duties under the Act;

[137] Section 3(1) of the 2003 Act.
[138] We must also have regard to any other principles appearing to us to represent best regulatory practice.
[139] Section 3(4A) of the 2003 Act.
[140] In relation to matters to which section 3(2)(g) is relevant. The 2003 Act sets out other matters to which Ofcom must, to the extent they appear to us relevant in the circumstances, have regard, in performing our duties. They include: the desirability of promoting competition and encouraging investment and innovation in relevant markets; the vulnerability of children and of others whose circumstances put them in need of special protection; the needs of persons with disabilities, the elderly and of those on low incomes; the desirability of preventing crime and disorder; the opinions of consumers and of members of the public generally; and the different interests of persons in the different parts of the UK and of the different ethnic communities within the UK. See Annex 1– Schedule 4 tests.

d) The need to exercise our functions to secure that providers may comply with such duties by taking or using measures, systems or processes which are proportionate to the size or capacity of the provider and the level of risk (and potential severity) of harm presented by the service;
e) The desirability of promoting the use of technologies which are designed to reduce the risk of harm to citizens; and
f) The extent to which providers demonstrate, in a way that is transparent and accountable, that they are complying with their duties.

A1.15 In line with our additional duties under the 2003 Act,[141] we have also considered the vulnerability of children and of others whose circumstances put them in need of special protection. We have considered:

a) The needs of disabled people, older people, and of those on low incomes;
b) The opinions of consumers and of members of the public generally;
c) The interests of persons in the different parts of the UK; and
d) The interests of the different ethnic communities within the UK.

Schedule 4 and additional Illegal Content Codes considerations

A1.16 The Act sets out that Ofcom must consider the appropriateness of the measures we recommend to different kinds and sizes of services and to providers of differing sizes and capacities.[142]

A1.17 We must also have regard to the principles that:

a) Providers must be able to understand which measures apply to their service;
b) The measures must be sufficiently clear, and at a sufficiently detailed level, that providers understand what they entail in practice;
c) The measures must be proportionate and technically feasible; and
d) The measures must be proportionate to our assessment of the risk of harm presented by services of that kind or size.

A1.18 We must also ensure that the measures described in the Codes are compatible with the pursuit of the list of online safety objectives set out in Schedule 4, and that we include measures relating to each of the areas specified in sections 10(4) and 27(4) (concerning illegal content).

A1.19 Under the 2003 Act, we are also required to conduct impact assessments when preparing a Code or amendment to a Code, including an assessment of the impact on small and micro-businesses.[143]

A1.20 We consider that assessing measures based on our impact assessment criteria is the right approach to ensuring the Codes protect UK users from illegal content while also protecting their rights and enabling service providers to operate and innovate in the market.

The Deregulation Act 2015

A1.21 Ofcom is required, when exercising our regulatory functions, to have regard to the desirability of promoting economic growth, including through considering the importance

[141] Section 3(4) of the 2003 Act.
[142] Schedule 4 of the Act.
[143] Section 7 of the 2003 Act, as amended by section 93 of the Act.

of ensuring the regulatory action we take is necessary and proportionate.[144] This duty is referred to as the "growth duty".

A1.22 We are also required to have regard to the Government's statutory guidance on the growth duty.[145] That guidance explains that the duty needs to be considered alongside our other statutory duties, and that its purpose is not to achieve or pursue economic growth at the expense of necessary protections.[146] Among other things, it also identifies particular drivers of economic growth, including innovation, investment and competition.

A1.23 The growth duty has applied to our online safety functions since 6 April 2026, following the end of a time-limited exclusion for these functions. We have therefore considered the wider economic impacts of our decisions (see annex 2, paragraphs 4.11-4.14).

[144] Section 108 of the Deregulation Act 2015.
[145] Section 110(3) of the Deregulation Act 2015.
[146] Department for Business and Trade, 2024. Growth Duty: Statutory Guidance – Refresh. [accessed 6 May 2026].

A2. Statutory tests and impact assessments

A2.1 This annex outlines our assessment of the relevant statutory tests and impact assessments Ofcom is required to carry out for all the decisions in this Statement. The primary reason for these decisions is to give effect to recent changes in the law which amend certain non priority offences to priority offences.

Statutory tests

A2.2 We consider our decisions are consistent with the general principles and objectives for Codes of Practice contained in Schedule 4 of the Act and section 3 of the Communications Act 2003. We explained in Chapter 14 of the December 2024 Statement why our Illegal Content Codes satisfied these principles and objectives. We consider that reasoning to apply here, and that the statutory tests are met by these decisions. We are not making changes to the substance of the measures. Instead, the decisions set out in this Statement change how some of the measures apply.

A2.3 We have also had regard to the principles in paragraph 2 of Schedule 4 and consider our decisions to be compatible with the pursuit of the online safety objectives: we consider our decisions to be clear as to their application; sufficiently clear and detailed for providers to understand what the decisions entail in practice; proportionate and technically feasible for the providers in scope; and that the extension of their application will ensure a higher standard of protection for children than adults on the services in scope.

A2.4 Chapter 14 of the December 2024 Statement also explained why we considered our Illegal Content Codes to be consistent with our general duties under the Communications Act 2003. We also consider that reasoning to apply here and that these duties are met by our decisions. In particular:

a. We consider our decisions to be consistent with our general duty to further the interests of citizens in relation to communication matters, and further the interests of consumers in relevant markets, including where appropriate by promoting competition, by aligning self-harm and cyberflashing with other priority offences.[147]

b. We also consider they secure the adequate protection of citizens from the harm presented by content on regulated services, through providers using appropriate systems and processes designed to reduce the risk of harm.[148]

c. In making these decisions, we have had regard to the principles that regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed[149] – the reasons for our decisions, and why we consider them to be necessary and appropriate, are set out in Section 3 of this Statement.

[147] Section 3(1) of the Communications Act 2003.
[148] Section 3(2)(g) of the Communications Act 2003.
[149] Section 3(3) of the Communications Act 2003.

d. Further, we have had regard to the factors as relevant set out in section 3(4A) of the Communications Act 2003, in particular the need for a higher level of protection for children than for adults.

e. We have also considered the vulnerability of children and of others whose circumstances put them in need of special protection.[150]

Impact assessment

A2.5 Ofcom is required by the Act to provide the following regulatory documents and guidance in respect of illegal content: the Risk Assessment Guidance and Risk profiles, the Register of Risk, the Illegal Content Judgements Guidance, the Codes of Practice and the Recordkeeping and Review Guidance. As we have discretion over the nature of these documents, we have carried out an impact assessment, as defined in Section 7 of the Communications Act 2003. In this context, we have considered the potential impacts of the decisions on economic growth. [151] We included this assessment in the March 2026 Consultation, particularly in Section 3 and Annex A1

A2.6 We have considered the potential impacts of our decisions on users and service providers, including small and micro-businesses. To the extent additional costs arise from our decisions, these are likely to be incremental and outweighed by the benefits to users in terms of protections from the risks of harm arising from the newly designated priority offences and also benefits to providers from having updated regulatory documents and guidance to assist them to comply with their legal duties under the Act. Overall, we consider that our approach is proportionate, including for small and microbusinesses. Moreover, we do not consider that the decisions are likely to have a significant adverse impact on economic growth. [152]

Combined impact assessment

A2.7 In section 3 of the March 2026 Consultation, we set out our assessment of the impact of each Codes measure applying to the new priority offences, encouraging or assisting serious self-harm and cyberflashing. We did not receive any substantive comments on our impact assessment, or our assessment of the cumulative impact. We set out our combined impact assessment below.

A2.8 Each measure delivers distinct benefit by targeting a different mechanism through which users encounter content. In this section, we set out the cumulative impact of the decisions relating to the Codes taken together and explain why, seen in the round, we consider the package of measures to be proportionate. We consider the cumulative impact on large services as well as on smaller services, that may become multi-risk as a result of our proposals.

---

[150] Section 3(4) of the Communications Act 2003.

[151] Our duties include having regard to the desirability of promoting economic growth (section 108(1) of the Deregulation Act 2015). The growth duty applies to Ofcom's exercise of its regulatory functions, which include online safety functions.

[152] The decisions are expected to result in incremental compliance costs for regulated services rather than introducing wholly new obligations. For services newly brought into scope of the measures, the costs incurred reflect the application of an existing regulatory framework to harms that have the same statutory standing as those already covered. We also consider that spillover effects on adjacent markets and the wider economy are unlikely to be significant.

A2.9 In the March 2026 Consultation, we provide more detailed impact analysis where specific measures could plausibly bring additional services into scope for the first time, or could require action in relation to each priority harm, which can create incremental work for services already implementing the Codes.

Impact on users

A2.10 Overall, we expect net positive impacts on user safety from applying a consistent package of protections to the two new priority offences. The measures act on complementary parts of the risk chain: governance, detection and moderation, recommender systems and search, reporting and crisis support, and user controls. Taking these together should reduce the likelihood and duration of exposure to illegal self-harm and cyberflashing content.

A2.11 We did not identify additional adverse impacts on users' rights beyond those already considered in the December 2024 Statement and April 2025 Statement, given that the decisions set out in this statement align application of existing protections to newly designated priority offences.

Impact on services

Services already subject to the Codes measures

A2.12 For providers already implementing the relevant measures, we expect limited incremental costs in the round. Many measures already do not require harm-by-harm implementation; where they do, the additional steps typically involve administrative updates – for example, ensuring tracking and analysis explicitly capture cyberflashing and serious self-harm, or confirming that moderation policies and prioritisation criteria encompass the new offences. We expect providers to integrate these updates into existing compliance cycles, rather than undertake separate projects for each measure, so the cumulative cost is likely to be lower than the sum of individual updates considered in isolation.

A2.13 We recognise potential path-dependency: some providers may previously have chosen to implement measures on a harm-specific basis (e.g. detailed policy chapters or training modules by harm). In those cases, amendment costs may be higher than a purely generic approach. However, such choices are not required by the Codes; providers retain flexibility to implement measures in ways proportionate to their service and risk profile. We therefore continue to consider incremental costs proportionate, given the expected user safety benefits.

A2.14 Costs are likely to scale with the size of the services. However, so does the potential to benefit users by preventing them from encountering material related to the new priority illegal harms. Larger services are also likely to have greater technical resources, which would help to limit costs.

Services becoming subject to the Codes measures as a result of our proposed changes

A2.15 A small number of services could newly come within scope where inclusion of the new offences changes a service's risk profile (e.g. becoming multi-risk) or where a measure applies because the service has the relevant characteristics (e.g. large services with specific functionalities for ICU J1/J2, or services conducting on-platform testing of recommender systems for ICU E1). For those services, the costs would be comparable to the costs assessed when the measures were first introduced, noting that many providers will already

have analogous systems in place for other harms – including under the Protection of Children Codes – thereby limiting incremental effort.

Rights assessment

A2.16 We consider the rights impact of our decisions is in line with the position set out in our March 2026 Consultation.

A2.17 Ofcom is required by section 6 of the Human Rights Act 1998 to act in a way which is compatible with the European Convention on Human Rights. In the March 2026 Consultation, we set out our approach to assessing the impact of our measures on human rights was the same as our approach set out in our December 2024 Statement and April 2025 Statement. These impacts are set out in Section 3 of the March 2026 Consultation.

A2.18 We did not receive stakeholder comments on our rights assessment.

A2.19 We do not consider our decisions in this Statement to have any additional impact on users' rights.

Equality impact assessment

A2.20 The purpose of our Equality Impact Assessment is to assess the likely impact of these decisions on individuals and communities with protected characteristics, in accordance with Ofcom's legal obligations under the Communications Act 2003, the Equality Act 2010 and the Northern Ireland Act 1998.

A2.21 We did not receive stakeholder comments on our Equality Impact Assessment.

A2.22 In preparing this Statement, we have had regard to the potential impacts of our decisions on people sharing protected characteristics (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation; and, in Northern Ireland, dependants and political opinion). In particular, due to overlap with the protected characteristics in the Equality Act 2010 and the Northern Ireland Act 1998, we have had regard as part of our Equality Impact Assessment to the vulnerability of those whose circumstances put them in need of special protection and the needs of persons with disabilities and of the elderly.

A2.23 The changes under this Statement are to reflect that the government has made to the offences of cyberflashing and encouraging or assisting serious self-harm and are designed to reduce the risks of harm relating to self-harm and cyberflashing online. We consider these decisions will primarily have positive impacts for people with protected characteristics – and in particular women and girls, including women and girls of ethnic minority groups, LGBTQ+ groups and children.

A2.24 We do not consider that the decisions will have negative impacts on equality of opportunity or the fostering of good relations. We have considered the different interests of persons in different parts of the UK but note that the measures apply to the UK as a whole. We have also had regard to the different interests of persons living in urban and rural areas, but we do not consider that there is any relevant difference in these interests for the purpose of our decisions. We have considered the impacts of our measures on different demographics, including those on low incomes, and the different interests of different ethnic communities within the UK, as these indirectly impact on groups with protected characteristics.

Welsh language impact assessment

A2.25 The Welsh language has official status in Wales. To give effect to this, certain public bodies, including Ofcom, are required to comply with Welsh language standards.[153] Accordingly, we have considered:

• the potential impact of our decisions on opportunities for persons to use the Welsh language;

• the potential impact of our decisions on treating the Welsh language no less favourably than the English language; and

• how our decisions have been formulated to have, or increase, a positive impact; or not to have adverse effects or to decrease any adverse effects.

A2.26 We did not receive stakeholder comments on our Welsh Language Impact Assessment.

A2.27 In making our decisions in this Statement, where relevant and to the extent we have discretion to do so in the exercise of our functions, we have considered the potential impacts on opportunities to the Welsh language and treating the Welsh language no less favourably than English.

A2.28 We do not expect our decisions to affect the opportunities for persons to use the Welsh language or to treat the Welsh language any less favourably than the English language. We do not consider that there is scope, acting within our powers, to formulate our decisions differently so as to have increased positive effects on these matters.

[153] The Welsh language standards with which Ofcom is required to comply are available on our website here.