Crisis response protocol

Online Safety – Additional Safety Measures

Statement

Published 09 June 2026

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

Contents

Section

Annex

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.

1.2 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 providers of regulated services likely to be accessed by children are required to take steps to prevent and protect children from encountering content harmful to children. Under the Act, Ofcom has duties to produce regulatory documents and guidance to assist providers. These include Codes of Practice (Codes) which set out the measures recommended for providers to comply with relevant duties.

1.3 In our June 2025 Additional Safety Measures Consultation (June 2025 Consultation), we consulted on a number of additional safety measures to include in our Codes, including that certain providers should have a crisis response protocol in place.

1.4 Given the speed at which online harms can escalate during a crisis, and the serious risks this can pose to public safety, we have decided to accelerate our work on these crisis response measures to ensure that services can begin to take appropriate steps in relation to these measures.

1.5 After careful consideration of stakeholder feedback, we have decided to include these crisis response protocol measures in our Codes.

1.6 Under these measures, service providers should prepare and apply a protocol to mitigate and manage the risks arising from a significant increase in relevant illegal content and/or content harmful to children on their services. The protocol should also, where applicable, address the increased risk of the service being used for the commission or facilitation of a priority offence during a crisis.

1.7 We have also decided to specify that when a crisis is determined to be occurring or likely to occur, certain service providers should establish a direct channel of communication through which crisis-related information may be shared by law enforcement agencies.

1.8 As we set out in Chapter 3: 'Crisis response', evidence suggests that illegal content and/or content harmful to children stemming from crises can pose an imminent risk to people both online and offline. During a crisis, there may be an increase on services in both the volume of illegal content and/or content harmful to children. There may also be an increase in the risks presented by such content, including the risk that services will be used to commit or facilitate a priority offence. The measures are intended to help mitigate and manage the risks arising from a significant increase in relevant content appearing on services during a crisis.[1]

1.9 They are also intended to ensure that service providers within scope can act promptly and effectively during a crisis. Having a crisis response protocol ensures services have contingency plans in place that enable rapid and coordinated action when a crisis emerges.

[1] See Chapter 3: 'Crisis response' for evidence and reasoning.

Without this, providers may lose valuable time identifying a crisis, assembling personnel, and developing an appropriate response. Our objective is that the rapid deployment of a temporary, cross-functional crisis response team will improve the speed at which issues across the service are identified and addressed.

1.10 We consider that having a dedicated law enforcement communication channel during a crisis will enhance the speed and reliability of information exchange, supporting faster risk mitigation and more coordinated public safety efforts.

1.11 Finally, we consider it important that crisis response protocols evolve and improve over time. Our measures state providers should conduct and keep a record of the post-crisis analysis, which should include analysis of the protocol's effectiveness. This would also mean we can formally request this report if necessary for the performance of our regulatory duties.

1.12 This statement sets out the reasoning for our decisions in relation to the crisis response measures. We expect to publish our decisions in relation to the majority of the other additional safety measures proposed in our June 2025 Consultation in Autumn 2026.

What is a crisis?

We have defined a crisis as an "an extraordinary situation in which there is a serious threat to public safety in the UK", which is highly likely to have resulted from a significant increase in relevant content or to have caused or cause a significant increase in relevant content.

During a crisis, certain kinds of illegal content and/or content harmful to children can spread rapidly online. In some cases, this can create significant risks to public safety in the UK. Evidence from previous crises has shown how perpetrators use online services in a variety of ways to carry out illegal activity such as inciting racial or religious hatred, making threats, or inciting violence. Not only can this lead to an increase in the amount of illegal content circulating online but it can result in violence offline.

Such crises are exceptional, and this means that online service providers' usual moderation measures may not be sufficient in these circumstances.

What decisions have we made?

Number in Codes	Measures	Who should implement this
ICU C15	The provider should prepare and apply an internal crisis response protocol. It should also conduct and record a post-crisis analysis.	Providers of large user-to-user services that are medium risk and providers of user-to-user services of any size that are high risk for relevant harms.

Number in Codes	Measures	Who should implement this
PCU C11		Providers of large user-to-user services that are likely accessed by children that are medium risk and providers of user-to-user services of any size that are likely accessed by children and are high risk for relevant harms.
ICU C16	Providers should implement a dedicated communication channel by which law enforcement can contact them on crisis-related matters during a crisis.	Providers of large user-to-user services that are medium risk or high risk for relevant harms.
PCU C12		Providers of large user-to-user services that are likely accessed by children that are medium risk or high risk for relevant harms.

Next steps

1.13 The amendments to the Illegal content Codes of Practice for user-to-user services and the Protection of Children Code of Practice for user-to-user services described in this statement will be implemented separately.

1.14 We have published draft consolidated versions of the relevant Codes incorporating the draft amendments that Ofcom intends to submit to the Secretary of State.

1.15 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. Introduction

The Online Safety Act 2023 and the user-to-user Codes of Practice

2.1 As set out in Chapter 1, the Act imposes a range of duties on service providers, and Ofcom is required to produce Codes for compliance with illegal content safety duties, reporting and complaints duties, and for compliance with children's online safety duties for providers of services likely to be accessed by children.[2]

2.2 While providers are not required to adopt the measures set out in the Codes, providers that do so will be treated as compliant with the duties to which they relate.[3]

2.3 We published the first Illegal Content user-to-user Codes in the December 2024 Statement on Protecting People from Illegal Harms Online (December 2024 Statement).[4] We published the first Protection of Children user-to-user Code in the April 2025 Statement on Protecting Children from Harms Online (April 2025 Statement).[5] In April 2025 and June 2025, we consulted on several additional safety measures, including that certain service providers put in place an effective crisis response protocol.

2.4 We will be amending both user-to-user Codes to include measures on crisis response (see paragraph 1.13). We designed the measures to strengthen service providers' responses to crises and to complement existing content moderation measures set out in our user-to-user Codes.

2.5 We provide more detail on the statutory basis of Ofcom's role and the issues we must consider when preparing Codes in Annex 2: Legal Framework.

Our approach to impact assessments for the measures

2.6 In designing our measures, we conducted an impact assessment to determine the proportionality of recommending that (i) some service providers have a crisis response protocol in place, and (ii) that some service providers should establish a dedicated communication channel for law enforcement during a crisis.

2.7 We have considered the following factors:

a) the prevalence and impact of harm;

---

[2] Part 3 of the Act places duties on providers of regulated services. These include duties set out in section 10 of the Act that require providers of regulated user-to-user services to take or use proportionate measures relating to the design or operation of the service to (among other things) prevent users from encountering priority illegal content. Priority illegal content is content that amounts to an offence specified in schedules 5, 6 or 7 of the Act (which includes terrorism, hate, harassment, stalking, threats and abuse, and foreign interference). Section 12 of the Act also places duties on providers of regulated services likely to be accessed by children to take steps to protect children from content harmful to children. Priority content (PC) that is harmful to children includes, but is not limited to, hate and abusive content and violent content.

[3] Section 49(1) of the Act.

[4] Ofcom, 2024. Protecting People from Illegal Harms Online.

[5] Ofcom, 2025. Protecting Children from Harms Online.

b) the efficacy of the measures to combat the harm (and, by extension, the benefits the measures would deliver);
c) the associated costs and impacts, including rights impacts, of the measures;
d) any risks associated with the measures; and
e) the scope of applicable service providers.

2.8 This remains consistent with our approach in the December 2024 Statement and the April 2025 Statement.

2.9 Following our online safety functions becoming subject to the growth duty in April 2026, we have also considered the potential impact of the measures on growth – both as individual measures and as part of our combined impact assessment alongside existing measures. [6]

2.10 The impact assessment for these measures is cumulative. This means we considered the anticipated impacts, costs, and benefits of the measure over and above those that result from existing measures.

2.11 We thank stakeholders for their feedback across the June 2025 Consultation.[7] We have addressed points that are specific to the measures in the relevant sections of Chapter 3, and general stakeholder feedback is addressed in Annex 1: Further stakeholder responses. We have considered all stakeholder responses received even where we have not referred to or quoted them in this statement.

Structure of this document

2.12 This statement includes the following main chapters that set out our reasoning for the final decisions:

- Chapter 1: 'Overview', gives a high-level summary of our decisions;
- Chapter 2: 'Introduction', outlines our approach to impact assessments for the measures and the structure of the statement and corresponding documents;
- Chapter 3: 'Crisis response', sets out our measures and reasoning.

2.13 This statement also includes 5 annexes:

- Annex 1: Further stakeholder responses
- Annex 2: Legal framework
- Annex 3: Statutory tests and impact assessments
- Annex 4: Further detail on economic assumptions and analysis
- Annex 5: Glossary

2.14 We have published our draft amended Codes separately:

- Draft consolidated Illegal content Codes of Practice for user-to-user services.
- Draft consolidated Protection of Children Code for user-to-user services.

[6] See Annex 3: Legal Framework 'The Deregulation Act 2015' for a description of this duty and how it applies to our Codes.

[7] Ofcom has also had careful regard to advice received from our Advisory Committees.

3. Crisis response

Introduction

3.1 In this chapter, we set out the detail of our decisions to include a new set of measures which are designed to ensure that in-scope services have an effective crisis response protocol in place, and for large in-scope services to have a dedicated communication channel with law enforcement during a crisis.

3.2 We consulted on proposals for these measures in our June 2025 Consultation. In this chapter, we address the feedback we received to our proposals and set out our final decision, along with our reasoning.

Measures on crisis response

3.3 In our June 2025 Consultation, we proposed measures setting out that user-to-user service providers should prepare and apply a written internal protocol for identifying and responding to a crisis. This included addressing the risk of an increase in illegal content and/or content harmful to children on their services during a crisis and (where relevant) mitigating and managing the risk of the service being used for the commission or facilitation of a priority offence.

3.4 We proposed to define a crisis as "an extraordinary situation in which there is a serious threat to public safety in the UK", either:

a) as a result of a significant increase in relevant illegal content/relevant content harmful to children on the service; or
b) which has caused or is highly likely to cause a significant increase in relevant illegal content/relevant content harmful to children on the service.[8]

3.5 We also proposed that once a crisis has ended or 90 days after it has begun, whichever comes first, providers should conduct a post-crisis analysis.

3.6 We proposed that providers of large services in scope should implement a dedicated communication channel by which law enforcement can contact them on crisis-related matters during a crisis.

3.7 We proposed the crisis response measures apply to:

a) providers of large user-to-user services that are medium risk, and providers of user-to-user services of any size that are high risk, of any one of the following priority illegal harms: terrorism, hate, harassment, stalking, threats and abuse, and foreign interference; and
b) providers of large user-to-user services that are likely to be accessed by children that are medium risk, and providers of user-to-user services of any size that are likely to be

[8] To the extent that our measures relate to illegal content, we are inserting them into the Illegal Content user-to-user Codes. To the extent they relate to content harmful to children, we are inserting the measures into the Protection of Children user-to-user Code.

accessed by children and are high risk of any one of the following harms: abuse, hate, and violent content.[9]

3.8 Throughout this chapter, where we use the term 'relevant illegal content', we refer to illegal content connected with the priority illegal harms in scope of this measure: terrorism, hate, harassment, stalking, threats and abuse, and foreign interference.

3.9 Where we refer to 'relevant content harmful to children', we refer to content harmful to children in scope of this measure: abuse, hate, violent content.

3.10 When combined, we refer to them as 'relevant content' or 'relevant harms'.

Our decision

3.11 Having considered all the stakeholder feedback, we have decided to broadly confirm the measures we proposed in our June 2025 Consultation, subject to the following amendments:

- Specifying that service providers should consider a public statement notice given to them by Ofcom, as directed by the Secretary of State under section 175 of the Act, in addition to their crisis indicators when determining whether a crisis is occurring or is likely to occur.[10] Section 175 of the Act provides that the Secretary of State may give a direction to Ofcom if they have reasonable grounds for believing that circumstances exist that present a threat to the health or safety of the public, or to national security. Such a direction may require Ofcom to give a public statement notice to a specified provider of a regulated service, or providers of regulated services generally.
- Clarifying the explicit objective for the crisis response protocol i.e., to mitigate and manage the risks arising from a significant increase in content which is illegal and/or harmful to children on the service during a crisis and, where relevant, the increased risk of the service being used for the commission or facilitation of a priority offence. This is to ensure that providers develop and implement their protocols in alignment with this objective.
- Clarifying that providers should activate the reactive aspects of their crisis response protocol (for example, the deployment of a crisis response team and the relevant systems and processes to address the risks posed by the crisis) as soon as reasonably practicable once a provider has determined that a crisis is occurring or is likely to occur, so that the crisis is swiftly managed.
- Clarifying that providers should record key decisions in their post-crisis analyses.

3.12 We have also decided to separate the dedicated communication channel for large services with relevant harms into its own separate measures.

---

[9] The violent content in scope of these measures are: content which encourages, promotes, or provides instructions for an act of serious violence against a person; and content which (1) depicts real or realistic serious violence against a person or (2) depicts the real or realistic serious injury of a person in graphic detail. See Chapter 8 of our Guidance on Content Harmful to Children.

[10] A 'public statement notice' is a notice requiring a provider of a regulated service to make a publicly available statement, by a date specified in the notice, about steps the provider is taking in response to the threat to the health or safety of the public, or to national security.

3.13 To contextualise these amendments, we have published the draft consolidated Codes for user-to-user services, and the measures are referred to as ICU 15, ICU 16 and PCU 11 and PCU 12.[11]

3.14 Subject to the Parliamentary process, the measures will form part of our Codes of Practice on terrorism, other duties and Protection of Children.

How these measures work

3.15 The crisis response measures are designed to ensure providers act promptly and effectively when a crisis occurs.

3.16 The measures include the following recommendations:

- that service providers prepare and apply a written internal protocol for identifying and responding to a crisis. This includes mitigating and managing the risks arising from a significant increase in the relevant content on the service during a crisis and (where relevant) mitigating and managing the risk of the service being used for the commission or facilitation of a priority offence; and
- that large service providers set up a dedicated communication channel allowing law enforcement to contact them on matters related to the crisis. See paragraph 3.27 for more details.

3.17 There are several elements to these measures, which are explained in the following paragraphs.

Definition of a crisis

3.18 Our definition of a crisis means that service providers have a common starting point for determining when a crisis is occurring or is likely to occur on the service for the purpose of the measures. We have broadly kept the same definition as proposed in our June 2025 Consultation (and outlined in paragraph 3.4):

- A crisis is an extraordinary situation in which there is a serious threat to public safety in the UK which is highly likely to:
  - have resulted (in whole or in part) from a significant increase in relevant illegal content and/or content harmful to children on a service; and/or
  - have caused, or cause, a significant increase in relevant illegal content and/or content harmful to children on the service.

3.19 We clarify that the "extraordinary situation" need not affect the whole of the UK to constitute a crisis; local or regional crises may still meet the definition. An overseas event may also meet the definition where it results in a serious threat to public safety in the UK, which is highly likely to have resulted (in whole or in part) from a significant increase of relevant illegal content and/or content harmful to children on a service, or which is highly

[11] In our June 2025 Consultation, the measure number ICU C16 was used for our measure on the availability of non-volunteer human moderators for livestreaming. We are still considering consultation responses in relation to this measure. We will re-number this as Measure ICU C17 if we decided to implement our consultation proposals.

likely to have caused or cause such an increase.[12] We intend this definition to capture exceptional occurrences on a service.

Internal crisis response protocol

3.20 Service providers should prepare and apply a written internal protocol for identifying and responding to a crisis. The protocol should set out how the provider will mitigate and manage the risks arising from a significant increase of relevant content during a crisis and, where relevant, the increased risk of the service being used for the commission or facilitation of a priority offence during a crisis. This protocol should include:

- indicators, identified by the provider, that the provider will consider in determining whether a crisis is occurring or is likely to occur;
- how the provider will regularly monitor those indicators to determine whether a crisis is occurring or is likely to occur;
- how the provider will keep the indicators under regular review to ensure that they remain the relevant indicators to be identified in their crisis response protocol;
- details of a crisis response team, including representatives of sufficient seniority from relevant internal teams, to facilitate timely decision-making and action;[13]
- how the provider will deploy the crisis response team as soon as reasonably practicable if the provider determines that a crisis is occurring or is likely to occur;
- systems and/or processes identified by the provider to mitigate and manage the risks arising from a significant increase in relevant illegal content and/or content harmful to children on the service during a crisis, and (where relevant) the risk of the service being used for the commission or facilitation of a priority offence, during a crisis; and
- how the provider will deploy the systems and/or processes as soon as reasonably practicable if the provider determines that a crisis is occurring or is likely to occur.

Examples of indicators and systems and/or processes that providers might include

Indicators

3.21 There are a range of indicators and systems and/or processes a service provider could put into place. The flexibility of these measures allows providers to determine those best suited to their service.

3.22 We set out a non-exhaustive list of indicators as examples of what a provider could choose to determine whether a crisis is occurring or is likely to occur. These include:

- external indicators:[14]
    i) information from law enforcement and/or other intelligence agencies;
    ii) information from NGOs or specialist organisations that are not trusted flaggers;
    iii) information from civil contingency bodies;
    iv) news reporting;

[12] This is an additional clarification since our consultation. See paragraph A1.3. for the stakeholder feedback that led to this addition.
[13] This is an additional clarification since our consultation. See paragraphs 3.43-.3.44 for the stakeholder feedback that led to this addition.
[14] Indicators i-v are an addition since our June 2025 Consultation. We explain the reasons for this addition in paragraph A1.80 where we discuss relevant stakeholder feedback on this point.

v) information from other services about emerging threats; or
vi) information from trusted flaggers.[15]

- internal indicators:

i) information obtained via complaints processes, such as increases in volume of complaints; or
ii) information obtained via content moderation processes, such as an increase in violative content as outlined in the service's terms of service.

3.23 Where the provider is subject to a public statement notice given by Ofcom under a direction issued by the Secretary of State pursuant to section 175 of the Act, the provider should consider this in addition to its indicators in determining whether a crisis is occurring or is likely to occur.[16]

Systems and/or processes

3.24 We set out a non-exhaustive list of systems and/or processes as examples of what providers might deploy during a crisis.

3.25 Relevant examples of systems and/or processes providers might deploy to mitigate and manage the risks arising from a significant increase in relevant illegal content and/or content harmful to children on the service and, where relevant, the risk of the service being used for the commission or facilitation of a priority offence may include, but are not limited to:

- Reallocating and/or increasing content moderation resources to meet the increase in illegal content and/or content harmful to children.[17]
- Adapting or providing additional guidance on content moderation policies if they do not effectively capture the type of content emerging from the crisis.[18]
- Proactively identifying the relevant content stemming from the crisis, either through:
  - proactive sweeps (a practice where human reviewers review trending/viral/illegal content stemming from the crisis);
  - keyword searching; or
  - other content moderation technology.

---

[15] A 'trusted flagger' is defined in Illegal Content user-to-user Codes in relation to measure ICU D14 "an entity which is a 'recommended trusted flagger' […] and any other person: a) whom the provider has reasonably determined has expertise in a particular illegal harm or harms; and b) for whom the provider has established a dedicated reporting channel". A trusted flagger is defined in paragraph 14.278 in Volume 4 of our April 2025) as "any entity for which the provider has established a separate process for the purposes of enabling the reporting of content which may include content harmful to children, based on the entity's experience".

[16] This is an addition since our June 2025 Consultation. We explain the reasons for this addition in paragraphs 3.46-3.47, where we discuss relevant stakeholder feedback on this point.

[17] This example reflects the existing resourcing measure in the Illegal Content user-to-user Codes (ICU C6) and the Protection of Children user-to-user Code (PCU C6). The respective measures recommend that in-scope providers resource their content moderation functions to give effect to their performance targets, having regard to (among other things) the propensity for external events to lead to an increase in demand for content moderation on the services.

[18] Our Illegal Content user-to-user Codes and Protection of Children user-to-user Code measures ICU C3 and PCU C3 recommend that providers should already have processes in place to update internal content policies in response to evidence of new and increasing harm on the services (as tracked in accordance with measures ICU and PCU A5). Therefore, providers in-scope of both these and the crisis response measures should already have the processes in place to be able to update policies in response to a crisis.

Responding to a crisis

3.26 Service providers should deploy the reactive elements of their crisis response protocol, i.e., their crisis response team and relevant systems and processes, as soon as reasonably practicable once they determine that a crisis is occurring (or is likely to occur) on their service.[19]

3.27 Providers of large in-scope services should, if they determine that a crisis is occurring or is likely to occur, implement a dedicated communication channel by which law enforcement can contact them on crisis related matters during a crisis.

3.28 We expect the channel to facilitate time-sensitive communication relevant to identifying and addressing illegal content and/or content harmful to children linked to a crisis. Law enforcement may provide service providers with urgent situational updates to support their response by helping them identify emerging trends that may not yet be visible on their services.

3.29 Our underlying assessment remains that a crisis response protocol should support more effective and efficient responses during a crisis. The dedicated law enforcement communication channel is designed to support this by streamlining urgent communication between large services and law enforcement, reducing delays and enabling clearer triage.

Post-crisis analysis

3.30 Once a crisis is over (or after 90 days since the provider determined that a crisis is occurring or was likely to occur, if sooner), providers should conduct and record a post crisis-analysis. This should include recording key decisions made during the crisis and assessing whether the crisis response protocol remains appropriate for mitigating and managing the risks arising from a significant increase in relevant content on the service during a crisis and, where relevant, the increased risk of the service being used to commit or facilitate a priority offence during a crisis.

3.31 We consider 90 days to be a reasonable period for providers to put in place more stable systems and processes once the initial demand associated with the crisis has lessened.[20]

3.32 A crisis should be treated as a short-term event, with crisis response protocols ending once the crisis criteria no longer apply (or after 90 days, whichever is sooner). Situations lasting beyond 90 days should shift from crisis response to 'business as usual' adjustments and longer-term resilience planning.

3.33 Providers should keep a record of the post crisis analysis. The relevant measures do not require services to submit the post-crisis analysis to Ofcom or publish it. However, we may request the analysis and its findings if necessary (for example, when exercising our regulatory supervision and/or enforcement functions).

3.34 We consider it appropriate for services to decide what information to include in their post-crisis analysis, so we have not specified this in the relevant measures. However, providers may consider including:[21]

---

[19] This is an additional clarification since our June 2025 Consultation. See paragraph A1.33 for the stakeholder feedback that led to this addition.

[20] For a detailed explanation of our decision, see paragraphs A1.36-A1.39 in the section of Annex 1 titled 'Threshold for ending a crisis'.

[21] This is additional guidance since our June 2025 consultation. See paragraphs A1.80 and A1.86 for the stakeholder feedback that led to this addition.

- a comprehensive decision log, documenting decisions (beyond the key decisions) taken during the crisis, including the rationale, timing and responsible teams;
- details of cross-functional teams involved in the crisis response, including roles and responsibilities;
- details of engagement with external partners, such as intelligence organisations, trusted flaggers or government;
- an account of the systems and processes deployed to manage the crisis, and any temporary adjustments made to business-as-usual operations; and
- lessons learned, such as:
  - whether the indicators used to identify the crisis were sufficient (including whether reliance on particular indicators – for example, news reporting alone – enabled timely activation);
  - whether resourcing was sufficient to address the crisis;
  - accuracy and effectiveness of the systems and processes that were deployed;
  - whether the crisis revealed gaps in existing internal policies or highlighted the need for updates; and
  - proposed changes to the overall operations of the service, such as including an additional indicator or team as part of the overall crisis response protocol.

Our reasoning

Effectiveness and benefits

3.35 As explained in our June 2025 Consultation, the crisis response measures are intended to ensure that service providers can act promptly and effectively during a crisis. The purpose of the measures is to help mitigate and manage the risks arising from an increase in relevant content appearing on services during a crisis.

3.36 Where relevant, these measures also aim to mitigate and manage the increased risk that a service will be used for the commission or facilitation of a priority offence by mitigating risks at each stage of an unfolding crisis.

3.37 We consider that providers having a crisis response protocol will ensure they have contingency plans in place, enabling rapid and coordinated action when a crisis emerges. Without this, providers may lose valuable time identifying a crisis, assembling personnel, and developing an appropriate response. This element of the measures is aligned with current industry best practice to an extent; there is evidence to show that some service providers already have some form of crisis response mechanisms in place.[22] However, we understand that not all service providers do so. The measures will therefore confer benefits by increasing the proportion of services that have crisis response protocols.

3.38 We consider it likely that the deployment of a temporary, cross-functional crisis response team will improve the speed at which issues across the service are identified and addressed. Such teams will also reduce the risk of communication failures and strengthen coordination under pressure, improving the provider's ability to rapidly identify and address an increase in relevant content on the service.

[22] UK Parliament, 2025. 25 February 2025 – Social media, misinformation and harmful algorithms – Oral evidence. [accessed 14 May 2026].

3.39 For large services, we consider that having a dedicated law enforcement communication channel during a crisis will enhance the speed and reliability with which law enforcement agencies can provide crisis-related information to services, supporting faster risk mitigation and more coordinated public safety efforts.

3.40 Finally, it is important that crisis response protocols evolve and improve over time. The inclusion in our measures of a post-crisis analysis following any crisis to review performance and identify opportunities to strengthen their future response will contribute to this aim.

3.41 Several stakeholders expressed general agreement, including with our assessment of the effectiveness and benefits of these measures set out in the June 2025 Consultation.[23] Five stakeholders disagreed with the measures, but no stakeholders provided evidence which called into question our assessment of the effectiveness and benefits of these measures.[24] All this considered, and taking account of relevant consultation responses, we have concluded that these measures will deliver significant benefits.

3.42 While stakeholder feedback has not led us to fundamentally revise our assessment of the benefits of these measures, there were stakeholders who disagreed with aspects of the measures, or who made recommendations for amendments to the measures. We discuss these responses in the following paragraphs.

Types of crises and harms in scope too narrow

3.43 Several civil society and industry stakeholders stated that Ofcom should broaden its crisis definition beyond violent events to include environmental disasters, pandemics, biomedical emergencies, and public health crises, citing examples from the Civil Contingencies Act 2004 (CCA) and the EU Digital Services Act 2022 (EU DSA).[25]

3.44 Some stakeholders recommended that additional harms should be in scope of the measures. The same stakeholders said that the measures should address misinformation

[23] Ofcom's Advisory Council for Northern Ireland response to the June 2025 Consultation, p.1; Center for Countering Digital Hate (CCDH) response to the June 2025 Consultation, p.3; Check My Ads Institute response to the June 2025 Consultation, pp.13-14; [✂]; Demos response to the June 2025 Consultation, pp.9-11; Department of Justice for Northern Ireland response to the June 2025 Consultation, pp. 15-16; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.17; Evangelical Alliance response to the June 2025 Consultation, p.13; Full Fact response to the June 2025 Consultation, p. 2; [✂]; Information Commissioner's Office (ICO) response to the June 2025 Consultation, p.31; [✂]; [✂]; National Center for Missing & Exploited Children (NCMEC) response to the June 2025 Consultation, p.9; National Police Chiefs' Council (NPCC) response to the June 2025 Consultation, p.16; Online Safety Act Network response to the June 2025 Consultation, p.28; Pinterest response to the June 2025 Consultation, p.6; [✂]; South West Grid for Learning (SWGfL) response to the June 2025 Consultation, p.7; [✂].

[24] Luethje, Y. response to the June 2025 Consultation, p.9; Mack, S. (Dr) response to the June 2025 Consultation, p 9; Name Withheld 4 response to the June 2025 Consultation, p.11; Name Withheld 26 response to the June 2025 Consultation, pp.10-11; Thompson, A. response to the June 2025 Consultation, p.10.

[25] British and Irish Law Education Technology Association (BILETA) response to the June 2025 Consultation, p.42; Demos response to the June 2025 Consultation, pp.26, 31; Full Fact response to the June 2025 Consultation, pp. 16-17; International Justice Mission response to the June 2025 Consultation, p.21; Molly Rose Foundation response to the June 2025 Consultation, p.17; Online Safety Act Network response to the June 2025 Consultation, pp.28-29; [✂]; [✂].

across all service types, including large services, search services, small high risk services, and generative AI.[26]

3.45 After considering this feedback carefully, we have decided not to broaden the measures to include additional types of crises or harms, for the following reasons.

- Under the Act, Ofcom is required to produce Codes of Practice setting out measures recommended for the purpose of complying with the illegal content safety duties and the children's safety duties. The definition of a crisis in the measures therefore refers to 'public safety' broadly, but only to the extent that the threat is highly likely to have resulted from, or to result in, a significant increase in relevant illegal content/content harmful to children on a service. Given the statutory purpose of Codes, it would not be appropriate for us to expand the measures to environmental disasters, pandemics or biomedical emergencies that do not have a direct link to illegal content and/or content harmful to children online. Expanding the crisis response measures to include these scenarios would stray beyond Ofcom's remit.
- Similarly, it would not be appropriate for us to address misinformation or disinformation in these measures where this does not amount to illegal content or content harmful to children as defined by the Act.
- We do not consider these measures the appropriate routes for addressing other types of harms – such as child sexual exploitation and abuse (CSEA), fraud, suicide and self-harm, and drugs – that fall outside the relevant harm in scope of these measures. These harms appear online persistently, and addressing them requires routine, long-term action. This is better managed through our existing measures rather than through a short-term intervention in response to a specific crisis.[27] The crisis response measures are designed to help service providers meet their current duties under the Act by ensuring they have clear processes for responding quickly and effectively to a crisis. As the measures are not designed to regulate day-to-day content moderation, we have decided not to expand the list of relevant harms. However, in the June 2025 Consultation we made a number of proposals designed to strengthen service providers' response to harms such as CSEA, fraud, and suicide and self-harm. We will publish a statement in Autumn 2026 setting out our decisions in relation to these proposals.
- Our decision to focus on user-to-user services reflects the evidence that these services pose the greatest risk during crises. The ability of such services to host user-generated content and enable rapid, widespread sharing means illegal content and/or content harmful to children can spread quickly and influence offline behaviour. In contrast, there is limited evidence on the role of search services in driving the same immediate or large-scale amplification of illegal content and/or content harmful to children. For this reason, we maintain that user-to-user services are the most appropriate focus of the measures.

[26] Barnardo's response to the June 2025 Consultation, p. 21; BILETA response to the June 2025 Consultation, p.42; Demos response to the June 2025 Consultation, p.9; Full Fact response to the June 2025 Consultation, pp.5-6; [✂]; International Justice Mission response to the June 2025 Consultation, p.21 ; Internet Watch Foundation (IWF) response to the June 2025 Consultation, pp.53-54; Kira, B. (Dr) response to the June 2025 Consultation, pp.12-14; Molly Rose Foundation response to the June 2025 Consultation, pp.17-18; NCMEC response to the June 2025 Consultation, p.9; SWGfL response to the June 2025 Consultation, p.22; Science, Innovation and Technology Committee response to the June 2025 Consultation, p.16; UK Finance response to the June 2025 Consultation, pp.16-17.

[27] Such as ICU C9 and ICU D14 in our Illegal Content user-to-user Codes.

- We acknowledge the feedback regarding generative AI services. Some generative AI services may, in certain circumstances, function as user-to-user services. In such cases, they may need to apply these measures if they fit the criteria on who the measures apply to. We will continue to monitor how these technologies evolve as part of our broader regulatory work.[28]

Section 175 directions

3.46 Two stakeholders queried how a direction given by the Secretary of State under section 175 of the Act would interact with the measures.[29] We agree that some directions given by the Secretary of State under section 175 of the Act will be relevant to how the measures operate. Clarifying the link between a direction under section 175 and our crisis response measures ensures providers consider public statement notices when judging whether a crisis is occurring or is likely to occur on their service.

3.47 We have therefore modified the measures to specify that service providers should consider a public statement notice issued to them (or to providers of regulated services generally) by Ofcom under a Secretary of State's direction under section 175 of the Act in addition to their crisis indicators when determining whether a crisis is occurring or is likely to occur. We explain the context of section 175 in paragraph 3.11 in the section 'Our decision'.

Impacts and costs

3.48 In our June 2025 Consultation, we set out estimates for the three main sources of costs associated with the measures: (1) preparing and applying a crisis response protocol; (2) preparing and deploying a crisis response team; and (3) conducting a post-crisis analysis.

3.49 We also set out that overall costs were likely to depend on several factors, such as existing systems and process, size, technical complexity, and risk for the relevant harms. We stated that the measures allow flexibility for providers to implement policies which are appropriate, accurate and proportionate to their service.

3.50 Stakeholder responses did not provide evidence that gave us reason to revise our cost estimates. We have only updated our cost estimates to reflect new Office for National Statistics (ONS) salary data since the June 2025 Consultation.[30] Further detail on stakeholder responses relating to costs is set out in Annex 1: Further stakeholder responses.

Preparing and applying a crisis response protocol

3.51 As set out in our June 2025 Consultation, providers will incur small one-off costs for preparing and applying a crisis response protocol, primarily labour costs to develop and agree the protocol.

3.52 We consider that it would take between 3 to 18 days to prepare and apply the crisis response protocol based on the service in question, with team size increasing with service size. We estimate this element could cost between £700 and £4,800 for a smaller service, and between £4,600 and £10,900 for a large service.[31]

---

[28] Ofcom. Open letter to UK online service providers regarding Generative AI and chatbots.
[29] Full Fact response to the June 2025 Consultation, p.17; Ofcom/DSIT meeting, 4 August 2025.
[30] See Annex 4 for further detail on economic assumptions and analysis.
[31] This is based on our assumption of between 3 to 10 days for smaller services and 10 to 18 days for large services of work from teams including individuals in professional occupations, with an additional four days of senior manager sign-off for large services. We note that in our consultation we incorrectly wrote "senior leader", but we applied the senior manager salary correctly. We have also split out the cost of establishing a

Establishing a dedicated communication channel with law enforcement

3.53 For large services also in scope of the measures to establish a dedicated communication channel with law enforcement, there will be additional costs from this component if they determine that a crisis is occurring or is likely to occur. We consider that the work to implement these measures could take up to 1 to 2 days of time from staff in professional occupations to set up the channel and cost between £200 and £1,000.[32]

Preparing and deploying a crisis response team

3.54 As set out in our June 2025 Consultation, costs will arise due to preparing and deploying a crisis response team, and teams will vary in size and composition across services. As these teams are likely to be primarily resourced from existing teams, the total incremental impact of them is expected to be minimal.

3.55 There will be costs associated with training the crisis team to familiarise themselves with the service's policies and processes in the event of a crisis. Based on our assumption of two days of training for each team member and estimating that small services could have one team member and large services could have 5 to 10 team members, we estimate this element could cost between £500 and £1,000 for a small service and between £2,600 and £10,100 for a large service.[33]

3.56 In the rare event of a crisis occurring there may be an opportunity cost associated with the reallocation of staff including content moderators to work on content stemming from the crisis, but we consider this proportionate to the risk being mitigated.

3.57 As set out in our June 2025 Consultation, we assume that service providers will adequately resource their content moderation functions to meet their existing safety duties.[34] We do not consider that these crisis response measures will mean services need to take a different approach to content moderation than that required by their safety duties.[35]

Conducting a post-crisis analysis

3.58 As set out in our June 2025 Consultation, a service affected by a crisis would incur costs to conduct a post-crisis analysis to analyse the service provider's response.

---

dedicated communication channel with law enforcement to the next paragraph. See Annex 4 for further detail on economic assumptions and analysis.

[32] We have split out this element of the cost of preparing and applying a crisis response protocol compared to how we presented the costs in our June 2025 Consultation. See Annex 4 for further detail on economic assumptions and analysis.

[33] For a large service we have assumed the crisis response team will be composed of two software engineering staff and the remainder staff in professional occupations. See Annex 4 for further detail on economic assumptions and analysis.

[34] See ICU C6 of the Illegal Content user-to-user Codes and PCU C6 of the Protection of Children user-to-user Code. These measures apply to (1) providers of large user-to-user services and providers of multi risk user-to-user services, and (2) providers of large user-to-user services and providers of multi risk user-to-user services likely accessed by children. It is theoretically possible that a single risk user-to-user service would be in scope of the crisis response measures, but not ICU C6 and PCU C6. However, we are not aware of services which would fall into this category and expect this will be a very small number (should any such services exist).

[35] See ICU C1, C2, C5 and C6 of our Illegal Content user-to-user Codes and PCU C1, C2, C5 and C6 of our Protection of Children user-to-user Code.

3.59 Based on our assumption that the core crisis response team will spend one week analysing the service provider's response, we estimate this element could cost between £1,200 and £2,400 for a small service and between £7,000 and £25,000 for a large service.[36]

Wider market impact

3.60 In our June 2025 Consultation we set out some of the wider market impacts which could occur, including that it may incentivise third-party trust and safety providers to develop crisis response protocols which could improve access and affordability of this for smaller providers.

3.61 One individual stakeholder said that smaller services struggling to comply risked market distortion and reduced innovation.[37]

3.62 These measures may impose costs on all in-scope services and may potentially have a more significant impact on smaller services. The only small services in scope are those at high risk of relevant harms. As evidence shows that such services can play an outsized role during a crisis, we consider that the cost burden for these small services is proportionate.[38]

Rights impact

Freedom of expression/freedom of association

3.63 Our assessment of the rights impact of these measures is broadly in line with the position set out in our June 2025 Consultation. We acknowledge that content moderation is an area in which the steps taken by services may have a significant impact on the rights of individuals and entities – in particular, to freedom of expression under Article 10 of the European Convention on Human Rights (ECHR), and privacy under Article 8. Given that the proposed crisis response measures are interconnected with, and enhance, existing content moderation measures, we have considered whether they are likely to result in interference with the rights of individuals and entities beyond the potential interference identified in connection with those existing measures, as set out in the December 2024 Statement and the April 2025 Statement.

3.64 We consider that the measures will not have a direct negative impact on users' freedom of expression and association. This is because the measures do not prescribe how providers should moderate content during a crisis. Instead, they require providers to have appropriate systems and processes in place. These systems should enable providers to act promptly and effectively to mitigate and manage the risks arising from a significant increase in the relevant illegal content and/or content harmful to children on the service during a crisis. Where relevant, they should also help providers mitigate and manage the increased risk that their service is used to commit or facilitate a priority offence.

3.65 However, we also recognise that there is a risk that providers may implement a crisis response protocol which prioritises speed of moderation over accuracy. This may result in a heightened risk of false positives (for example, content being removed from the service when it is not illegal content and/or content harmful to children). We recognise that, due to the types of content to which the measures relate, there is a risk that such content would contain the most highly protected forms of expression. This may include: religious

[36] See Annex 4 for further detail on economic assumptions and analysis.
[37] Turner, B. response to the June 2025 Consultation, pp.68-70.
[38] See paragraphs 3.82 – 3.86 in the section titled 'Size of service' for more information on the risks that smaller services pose during crises.

expression (which could also have an impact on users' rights to religion or belief under Article 9) or political speech, and expression in relation to content of democratic importance, journalistic content, and that from recognised news publishers.

3.66 We acknowledge that, where providers adopt such an approach, there is a potential for false positives to adversely impact users' rights under the ECHR, particularly Article 10. However, we note that the potential interference is to be balanced against the very significant public interest in moderation of relevant illegal content and/or content harmful to children during a crisis, particularly given that the risk of harm deriving from illegal content and/or content harmful to children may be very significant where there is a serious threat to public safety in the UK. We also note that crises, by our definition, are extraordinary situations which occur infrequently, and therefore that the interference is likely to arise only rarely. In this context, we consider that a higher risk of false positives is likely to be proportionate.

3.67 We reiterate that this approach is not what the measures recommend but is a potential outcome of the measures depending on how they are applied by service providers.

3.68 We also consider that the proposed measures could have positive impacts on the freedom of expression of users. The moderation of illegal content and/or content harmful to children during a crisis could result in safer spaces online where users may feel more able to join online communities and to receive and impart information which is of particular use to them in a crisis.

3.69 In the circumstances – and noting that services have discretion about what to put in their crisis response protocols – we consider that any interference with users' rights to freedom of expression is proportionate and is mitigated by the flexibility of the measures, which allow providers to balance speed and accuracy when implementing crisis response protocols.

3.70 Stakeholder feedback did not identify additional impacts in relation to rights that we had not already considered in our June 2025 Consultation, and we do not consider that the changes we are making to our proposals will have any additional impact on rights. Therefore, our assessment of the rights impact of the measures has not changed.

3.71 Some stakeholder comments indicated that they understood that the measures would enable Ofcom or the UK Government to declare a crisis or related to the introduction of "emergency powers".[39] These stakeholders were concerned about the impact of this on users' rights to freedom of expression. However, as set out in our June 2025 Consultation and in paragraph 3.21, the decision as to whether a crisis is occurring or is likely to occur (for the purpose of the measures) will be made by individual providers in relation to their own services. The measures do not enable Ofcom to declare a crisis, nor do they introduce emergency powers. They are intended to assist services in their preparedness for a crisis and to ensure that they can effectively and efficiently respond to a crisis affecting them. As explained in further detail at 3.23, while the measures recommend that providers consider a public statement noticed issued to them by Ofcom under the Secretary of State's

[39] [✂]; Francis, S. response to the June 2025 Consultation, p.16; [✂]; Klaushofer, A. response to the June 2025 Consultation, p.10; Name Withheld 4 response to the June 2025 Consultation, p.11; Name Withheld 26 response to the June 2025 Consultation, p.12; Name Withheld 27 response to the June 2025 Consultation, p.12; Porter, J. response to the June 2025 Consultation, p.9; Together Campaign response to the June 2025 Consultation, p.6.

direction (section 175 of the Act) in addition to their crisis indicators when determining whether or not a crisis is occurring or is likely to occur, this is not determinative of a crisis (for the purpose of these measures) occurring on the service in question.

Privacy

3.72 We have considered whether there were additional privacy and data protection impacts of the proposed measures to those identified in relation to the existing content moderation measures as set out in the December 2024 Statement.

3.73 Our assessment of this matter is broadly in line with the position set out in our June 2025 Consultation. We consider the privacy and data protection impacts of the proposed measures to be inextricably linked and have therefore assessed them together. We consider that the proposed measures would not result in any significant additional interference with users' rights to privacy under Article 8, or their rights under data protection law. Providers processing users' personal data will still be required to comply with applicable data protection legislation, including in relation to the accuracy of personal data. We consider the proposed measures to be compatible with privacy and data protection requirements. Overall, and taking the benefits to users and affected persons into consideration, we consider that any potential impact on privacy and data protection rights from the measures is proportionate.

3.74 One individual stakeholder expressed concern that the measures could increase privacy and data security risks through greater data collection.[40] While we agree in principle that increased personal data collection could potentially result in a greater risk to privacy and data protection rights, the measures do not recommend steps that would require greater personal data collection, and therefore we do not agree that this is a risk arising from the measures. As a result, we have not changed our assessment from the position set out in our June 2025 Consultation.

3.75 As acknowledged in paragraph 3.65, while not recommended by the measures, there is a potential for providers to adopt a crisis response protocol which prioritises speed over accuracy in respect of content moderation. This may present an increased risk of false positives, leading to the removal of content which is not illegal or harmful to children. There is therefore an associated risk of the creation of inaccurate personal data – for example, a record that a user has posted illegal content or content harmful to children. We reiterate that adopting an approach which prioritises speed over accuracy is not recommended by the measures, and that providers must continue to comply with their user privacy and data protection obligations when implementing and activating their crisis response protocol. Providers are also encouraged to have regard to the Information Commissioner's Office (ICO) guidance on content moderation, accuracy, and fairness obligations.

Who these measures apply to

3.76 In our June 2025 Consultation we proposed to apply these measures to:

a) providers of large user-to-user services that are medium risk, and providers of user-to-user services of any size that are high risk, for any one of the following priority illegal harms: terrorism, hate, harassment, stalking, threats and abuse, and foreign interference; and

[40] [✂].

b) providers of large user-to-user services that are likely to be accessed by children that are medium risk, and providers of user-to-user services of any size that are likely to be accessed by children and that are high risk, for any one of the following harms that are priority content harmful to children: abuse, hate, and violent content.[41]

3.77 We proposed to apply the measures to these harms because crises can exacerbate the risks of these harms occurring both online and offline. An example of this was the 2024 summer riots following the tragic attack in Southport, where online content fuelled nationwide unrest, spreading hatred and provoking violence against racial and religious groups.[42]

3.78 We proposed to apply these measures to large services with medium risk of the relevant harms as we considered that the benefits would be significant. It would ensure that these services, which can play a significant role in spreading relevant content during a crisis due to their reach, act swiftly to protect their large user base. While we recognised the potential impact on small service providers due to the associated costs, given the structural and outsized risk of small services during a crisis, we proposed to apply these measures to small services where they identified a high risk of relevant harms.[43] Given the limited evidence of the role that search services play during crises, we did not propose including them within the scope of these measures.

3.79 We received stakeholder feedback on the approach we had taken to assessing the proportionality of these measures which is included in Annex 1: Further stakeholder responses. We received feedback on the specific proportionality of applying these measures to smaller services, which we discuss in paragraphs 3.82 – 3.86.

3.80 We address our reasoning for applying these measures only to certain user-to-user services in response to stakeholder feedback in paragraph 3.45.

3.81 We received no feedback on our proposal to apply the measures to large services that pose a medium risk of the relevant harms.

Size of service

3.82 Several stakeholders said that the measures would impose high costs and disproportionate burdens on smaller services, especially small community services. They said that smaller services lacked the financial and operational capacity to implement the measures and that we had underestimated compliance costs and overestimated benefits, particularly given the rarity of crises. They warned that this could lead to service shutdowns, feature restrictions, or market withdrawal (thus concentrating power among large firms), and called for either a more flexible approach that scaled requirements to service size or for such services to not be in scope of the measures.[44]

---

[41] The violent content in scope of these measures is: content which encourages, promotes, or provides instructions for an act of serious violence against a person; and content which (1) depicts real or realistic serious violence against a person or (2) depicts the real or realistic serious injury of a person in graphic detail. See Chapter 8 of our Guidance on Content Harmful to Children. [accessed 6 May 2026].

[42] Institute for Strategic Dialogue, 2024. From rumours to riots: How online misinformation fuelled violence in the aftermath of the Southport attack. [accessed 3 March 2026]; Spring, M., 2024. Did social media fan the flames of riot in Southport? BBC, 31 July. [accessed 3 March 2026].

[43] See paragraphs 3.82 – 3.86 in the section titled 'Size of service' for more information on the risks that smaller services pose during crises.

[44] BILETA response to the June 2025 Consultation, p.42; [✂]; Demos response to the June 2025 Consultation, p.31; Francis, S. response to the June 2025 Consultation, p.14; [✂]; Klaushofer, A. response to the June 2025

3.83 We have carefully considered this feedback. However, we have concluded that it is important that smaller high risk service providers remain in scope of the measures. The dissemination of illegal and/or content harmful to children often begins on smaller services before spreading to larger ones, enabling perpetrator networks and inciting offline violence.[45] Some stakeholders made similar points, noting that smaller services identified as the 'weakest link' could potentially be a risk during crises.[46] This demonstrates the role of such services in the wider ecosystem of harm during crises, and thus the importance of small services which have identified a high risk of relevant harms being included in scope to increase the benefits of the measures.

3.84 Smaller in-scope services could benefit from having proportionate protocols in place ahead of time. This kind of preparation can help support a more timely and effective response in a crisis, particularly where there may be less flexibility to adapt quickly without prior planning.

3.85 Several factors help reduce costs for small high risk services under these measures. Protocols and review processes, such as varying indicators and monitoring methods, can be tailored to each service. Only what we consider to be the essential components of an effective crisis response are included in the measure, and law enforcement contact channels will be recommended solely for large services. Some of the costs of these measures will only be incurred in the event of a crisis occurring on a service, and services may be able to adapt existing frameworks to conform with the measures. In the event of a crisis, we envision that services will redeploy existing content moderation resources to handle them, rather than requiring new staff, which limits the financial impact.

3.86 Given the outsized role small services can play in a crisis and the flexibility of the measures, we consider that it is proportionate to apply these measures to smaller services at high risk for the relevant harms.

3.87 We have decided to apply the measures on preparing and applying a crisis response protocol, deploying a crisis response team and conducting a post-crisis analysis for:

- providers of large user-to-user services that are medium risk, and providers of user-to-user services of any size that are high risk, of any one of the following priority illegal harms: terrorism, hate, harassment, stalking, threats and abuse, and foreign interference; and
- providers of large user-to-user services that are likely to be accessed by children that are medium risk, and providers of user-to-user services of any size that are likely accessed by children and are high risk, of any one of the following harms that are priority content harmful to children: abuse, hate, violent content (instructions for an act of serious violence against a person), and violent content (person).

Consultation, p.4; [✂]; Name Withheld 26 response to the June 2025 Consultation, p.112; [✂]; UK Finance response to the June 2025 Consultation, p.17.

[45] Casciani, D., BBC Verify, 2024. Violent Southport protests reveal organising tactics of the far-right, BBC. [accessed 3 March 2026]; Schwieter, C, 2022 Online crisis protocols Expanding the regulatory toolbox to safeguard democracy during crises. [accessed 3 March 2026]; UK Parliament, 2025. Social media, misinformation and harmful algorithms.[accessed 19 May 2026]; Zheng, M., Sear, R., Illaria, L., Restrepo, N., and Johnson, N., 2024. Adaptive link dynamics drive online hate networks and their mainstream influence. npj Complexity, 1, 2. [accessed 5 May 2025].

[46] UK Finance response to the June 2025 Consultation, p.17.

3.88 As set out in paragraph 3.6 our measures on the implementation of a dedicated communication channel for law enforcement apply to:

- providers of large user-to-user services that are medium or high risk of any one of the following priority illegal harms: terrorism, hate, harassment, stalking, threats and abuse, and foreign interference; and
- providers of large user-to-user services that are likely to be accessed by children and that are medium or high risk of any one of the following harms that are priority content harmful to children: abuse, hate, violent content (instructions for an act of serious violence against a person), and violent content (person).

Combined impact assessment

3.89 In the previous section, we assessed the impacts of the crisis response measures on a standalone basis and concluded that they were proportionate. In this section, we consider the impact of the measures in combination with existing measures in the user-to-user Codes. In particular, whether these measures have distinct benefits to contribute to the overall package, and whether the overall impact on services is proportionate, particularly for smaller services.

3.90 Our June 2025 Consultation Combined Impact Assessment provisionally concluded that the proposed package of measures was proportionate. We received a range of views from stakeholders on this topic, including stakeholders who supported the assessment and those who disagreed with our package of measures. Some stakeholders specifically disagreed with our package of measures for smaller services, with some arguing it could place a disproportionate burden on smaller or low risk providers and create a negative impact on competition in the market. As this feedback relates to the whole package of measures which we proposed in our June 2025 Consultation, these responses will be addressed in more detail when we publish our Combined Impact Assessment as part of the statement for the remaining package of measures. However, we have considered these themes raised in respect of the measures in this statement.

3.91 Our view following our assessment of this feedback is that these measures for crisis response will offer additional benefits that do not substantially overlap with benefits from existing measures. These measures complement existing measures in the user-to-user Codes and provide additional important protections to users in the event of a crisis occurring on a service. We have taken a risk-based approach and only recommended these measures for smaller services when they are at high risk of relevant content. In these cases, we consider the cost of these measures to be proportionate to the benefits. We have concluded that the combined impact of the measures, when applied alongside the existing measures set out in the user-to-user Codes, is proportionate.

Growth duty

3.92 We have considered the impact of these measures, in addition to existing Code measures, further to our growth duty. While these measures are likely to increase regulatory compliance costs for service providers – including some smaller services – we consider that there is unlikely to be significant impact on innovation, investment, and competition. We also do not expect any significant adverse impact on adjacent markets or the wider economy from these measures.

3.93 We note that the measures are targeted at services which are at medium or high risk of types of illegal content or content harmful to children that are of particular concern during a crisis. The measures are expected to have a significant positive impact on safety, while our assessment indicates that any adverse effects on growth is likely to be minimal. After assessing the impact in light of the growth duty, and considering the wider economic impacts of our decision, we consider that recommending these measures is proportionate.

Conclusion

3.94 Our analysis suggests that the crisis response measures will provide substantial benefits for UK users. By ensuring that services can act quickly during times of crisis, the measures are designed to help mitigate and manage the risks arising from a significant increase in illegal content and/or content harmful to children on a service during a crisis and, where relevant, the risk that a service will be used to commit or facilitate a priority offence.

3.95 As noted in paragraphs 3.48-3.62 we expect the costs of these measures to be relatively minimal. This is supported by the flexibility we have built into the framework which allows providers to design and operate crisis response protocols that are proportionate to their service risk and size.

3.96 By reference to our consultation proposals, we have amended the measures to:

- Specify that service providers should consider a public statement notice given to them by Ofcom, as directed by the Secretary of State under section 175 of the Act, in addition to their crisis indicators when determining whether a crisis is occurring or is likely to occur.
- Clarify the explicit objective for the crisis response protocol i.e., to mitigate and manage the risks arising from a significant increase in content which is illegal and/or harmful to children on the service during a crisis and, where relevant, the increased risk of the service being used for the commission or facilitation of a priority offence.
- Clarify that providers should activate the reactive aspects of their crisis response protocol (for example, the deployment of a crisis response team and the relevant systems and processes to address the risks posed by the crisis) as soon as reasonably practicable once a provider has determined that a crisis is occurring or is likely to occur, so that the crisis is swiftly managed.
- Clarify that providers should record key decisions in their post-crisis analyses.

3.97 To contextualise these amendments, we have published the draft consolidated Codes of Practice for user-to-user services, and the measures are referred to as ICU 15, ICU 16 and PCU 11 and PCU 12.

3.98 Subject to the Parliamentary process, the measures will form part of our Codes of Practice on terrorism, other duties and Protection of Children.

A1. Further stakeholder responses

About this document

A1.1 This annex addresses the additional points that were made by respondents to our June 2025 Additional Safety Measures Consultation (June 2025 Consultation).

A1.2 While we have reviewed all the relevant feedback, we did not consider that the points set out in this Annex required substantial additions or explanations in this Crisis Response chapter.

Definition of a crisis

Definition is too vague

A1.3 In their response to the June 2025 Consultation, several stakeholders expressed the view that the definition of a crisis, and the specific terms within it, were too vague.[47] A number of stakeholders provided suggestions for more specificity.

A1.4 The National Police Chiefs' Council (NPCC) said different definitions of crisis may be needed for different circumstances and noted resource implications at every stage. It agreed providers should act and said policing aims to safeguard children and disrupt offenders. It suggested an iterative approach to build joint working and information-sharing processes supported by new technology.[48]

A1.5 Several stakeholders asked for clarity regarding terms used in our definition, expressing the view that wording like "extraordinary situation" and "serious threat to public safety" was vague and risked inconsistent interpretation.[49]

Our response

A1.6 As stated in our June 2025 Consultation, in developing our definition of a crisis, we considered several key factors, including the EU DSA definition of a crisis.[50]

A1.7 Our approach complements that set out in the EU DSA, supporting consistency and proportionality. We consider that the natural meaning of these terms is sufficient, and we do not intend to give a further definition.

A1.8 We do not consider it appropriate to adopt the Civil Contingency Act's (CCA) definition of a crisis, as the CCA's framework is primarily designed for offline emergencies which may not

[47] Antisemitism Policy Trust response to the June 2025 Additional Safety Measures Consultation (June 2025 Consultation), p.2; Barnardo's response to the June 2025 Consultation, p.21; Mack, S. (Dr) response to the June 2025 Consultation, p.9; Full Fact response to the June 2025 Consultation, pp.16-17; Demos response to the June 2025 Consultation, pp.25-27, 29; [✂]; Molly Rose Foundation response to the June 2025 Consultation, pp.17-18; Name Withheld 4 response to the June 2025 Consultation, p.11; Name Withheld 26 response to the June 2025 Consultation, p.12.

[48] National Police Chiefs' Council (NPCC) response to the June 2025 Consultation, p.17.

[49] Mack, S. (Dr) response to the June 2025 Consultation, p.9; [✂]; Name Withheld 4 response to the June 2025 Consultation, p.11; Name Withheld 26 response to the June 2025 Consultation, p.12.

[50] Article 36 states that; "a crisis shall be deemed to have occurred where extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it." Article 36 of the EU Digital Services Act, 2022.

involve the types of online harms or content-related risks that fall within the scope of our duties under the Online Safety Act 2023 (the Act).

A1.9 We consider that our approach supports consistency and ensures that the measures are proportionate overall. We have therefore decided to maintain the definition we set out in the June 2025 Consultation.

Clarifying crisis impact scope

A1.10 Four stakeholders said the crisis definitions needed clearer geographical scope.[51]

Our response

A1.11 Adding explicit references to specific locations, communities, systems or services would constrain the definition and risk excluding relevant scenarios, thereby limiting its adaptability over time.

A1.12 We have therefore not included explicit references to specific locations, communities, systems or services in the definition. In relation to the geographic scope of the crisis, see Chapter 3 paragraphs 3.18-3.19 in the section titled 'Definition of a crisis'.

Setting universal thresholds for "significant increase"

A1.13 Several stakeholders requested clear thresholds for determining what constitutes a "significant increase" in illegal content and/or content harmful to children.[52] The Online Safety Act Network raised concerns that Ofcom leaves services to set their own crisis indicators and said examples given are insufficient. It called for clearer standards on indicators, triggering protocols, and response speed to ensure consistency and prevent weaknesses in moderation from undermining the measures.[53] The British and Irish Law Education Technology Association (BILETA), in setting out a number of recommendations for the measures, said crisis thresholds should be high enough to justify enhanced proactive measures, such as temporarily overriding non-essential functionalities and defined by measurable events that immediately heighten risk, such as services being used to coordinate targeting of victims via AI or other means.[54]

Our response

A1.14 We do not consider it appropriate to define a universal threshold for a "significant increase" because the scale and trajectory of crises manifest differently across services and baseline volumes cannot be standardised across service type and size.

A1.15 However, providers should understand their own baseline levels of the relevant content identified on their services as part of their crisis response protocol. This enables them to discern what constitutes a "significant increase" from their baseline, which is a necessary part of our definition of a crisis.

A1.16 We recognise the systemic risks associated with offender behaviour shifting to encrypted environments and the emergence of hyper realistic AI generated illegal content. These are

[51] Ofcom's Advisory Council for Northern Ireland response to the June 2025 Consultation, p.3; Demos response to the June 2025 Consultation, p.26; Full Fact response to the June 2025 Consultation, pp.16-17; Online Safety Act Network response to the June 2025 Consultation, pp. 28-29; [✂].

[52] Demos response to the June 2025 Consultation, pp.16, 29; Molly Rose Foundation response to the June 2025 Consultation, pp.17-18.

[53] Online Safety Act Network response to the June 2025 Consultation, pp. 28-29.

[54] British and Irish Law Education Technology Association (BILETA) response to the June 2025 Consultation, p.41.

important concerns, and providers must take proportionate steps under their existing duties to mitigate such harms. However, the crisis response measures themselves do not recommend specific technologies as this would not be proportionate across all services. Providers remain responsible for selecting appropriate tools and approaches that are lawful, effective, and suited to their risk profile.

Disagreement with the definition

A1.17 An individual stakeholder said they disagreed with the proposals, stating the proposed measures would create a single point of failure for the entire UK internet, making it highly vulnerable to foreign interference or enemy action.[55]

Our response

A1.18 Our definition does not prescribe a single decision-maker, but aims to provide a common starting point for services on the types of situations that may warrant a crisis response. The definition was designed to support resilient and distributed crisis preparedness and response, ensuring providers put in place arrangements that are proportionate, robust and appropriate for their service.

Granting a single body the power to declare a crisis

A1.19 Some stakeholders expressed potential challenges around granting a single body – or services themselves – the power to declare a national crisis, noting this could concentrate power, undermine democratic principles, and erode public trust.[56]

Our response

A1.20 We acknowledge concerns raised about crisis declaration and aim to provide further clarity. The definition of a crisis as set out at paragraph 3.18 will always be service specific, and therefore one provider determining that a crisis is occurring or is likely to occur on its service does not necessarily mean that a crisis is occurring on any or all other in scope services. Nor do the measures give Ofcom, 'the state', or a service provider the power to officially declare a crisis (as per our definition) in the UK.

A1.21 While the measures recommend that providers consider a public statement noticed issued to them by Ofcom under the Secretary of State's direction (section 175 of the Act) in addition to their crisis indicators when determining whether a crisis is occurring or is likely to occur, this is not necessarily determinative of a crisis (for the purpose of these measures) occurring on the service in question, and this will be determined by the provider in light of their crisis response protocol and the suite of indicators it monitors in respect of its service.

A1.22 We also considered stakeholder suggestions for a democratically accountable body to declare a crisis or centrally monitor services. In our view, this is not feasible: no such body has round-the-clock access to services' internal data and granting this access would pose significant privacy and data-protection risks. Given these constraints, we are of the view

[55] Luethje, Y. response to the June 2025 Consultation, p.9.

[56] Demos response to the June 2025 Consultation, pp.14-15, 28, 31; Francis, S. response to the June 2025 Consultation, p.16; [✂]; [✂] Klaushofer, A. response to the June 2025 Consultation, p.10; Microsoft response to the June 2025 Consultation, p.13; Name Withheld 26 response to the June 2025 Consultation, p.12; Name Withheld 4 response to the June 2025 Consultation, p.11; Porter, J. response to the June 2025 Consultation, p.9; Together Campaign's response to the June 2025 Consultation, p.6; [✂].

that services are best placed to identify when crisis-related risks emerge on their own services, within the framework established by Ofcom.

A1.23 Crises affect services differently; relevant content may surge and spread rapidly on some services but barely appear on others, additionally it may also move unevenly between services. A centralised declaration of a crisis would not reliably capture these differences.

Introducing tiered levels to a crisis

A1.24 Some civil society stakeholders and individuals stated Ofcom should adopt a tiered approach to reflect varying severity levels of a crisis, using frameworks such as Full Fact's five-stage model.[57] One stakeholder also recommended tiered standards based on the size and risk of the service.[58]

Our response

A1.25 We do not consider Full Fact's framework to be an appropriate framework for these measures for the following reasons:

- Full Fact's framework provides a structured approach for managing information incidents and thus was designed to address a broader category of content than that set out in the duties on service providers in the Act.[59]
- Our crisis response measures are specifically developed to target the relevant content in extraordinary situations in which there is a threat to public safety in the UK.
- Since the scope and purpose of Full Fact's model differs from the objectives of our measures, it would not be appropriate to adopt the framework in this context.

A1.26 Our crisis response protocol 'stages' (pre, during, and post-crisis) are aligned with the crisis lifecycle model set out in 'The Amber Book – Managing Crisis in Central Government', which is the framework for how UK Central Government responds collectively to crises requiring coordinated action, and we are remaining with these stages for alignment.[60]

A1.27 More broadly, we consider that a tiered approach would not be appropriate for our measures for the following reasons:

- We acknowledge that certain events may fall outside of our definition of a crisis. And though these incidents may warrant attention, these measures are not intended to address events which are not extraordinary situations in which there is a serious threat to public safety in the UK.
- A tiered approach could risk the protocol becoming overly complex, introducing unnecessary distinctions between levels of crises and increasing the risks of delays in activating appropriate measures. Such complexity would undermine the intent of these measures,

---

[57] Demos response to the June 2025 Consultation, p.29; Full Fact response to the June 2025 Consultation, pp.6-7, 18-19; respondents citing: Full Fact, 2021. Framework for Information Incidents. [accessed 19 May 2026]; [✂]; Molly Rose Foundation response to the June 2025 Consultation, pp.17-18; Online Safety Act Network response to the June 2025 Consultation, p.29.

[58] [✂].

[59] Full Fact's definition of an information incident in their framework is "a cluster or proliferation of inaccurate or misleading claims or narratives, which relates to or affects perceptions of or behaviour towards a certain event or topic happening online or offline. This can occur suddenly or have a slow onset."

[60] Providers may, where appropriate, incorporate additional stages into their own internal protocols, provided the core three-stage structure is retained. Cabinet Office, 2026. The Amber Book – Managing Crisis in Central Government'. [accessed 19 May 2026].

which is to support timely and effective response to the types of events we are seeking to address.

- A tiered approach would also impose additional resource burdens on providers, particularly smaller providers, which would be required to monitor multiple categories of incidents and maintain differentiated responses for each. This would add operational complexity without clear evidence that it would lead to more effective outcomes.
- We have taken into consideration the size and risk level of services in determining providers in scope of these measures, as set out in Chapter 3: paragraphs 3.76-3.88 in the section titled 'Who these measures apply to'. The measures only apply where we consider they are proportionate, based on the service's size and risk profile. For services in scope, the framework provides flexibility to develop crisis response protocols that reflect their operational models and risks. Given the evidence that smaller services can play a significant role in the dissemination of illegal content and/or content harmful to children during crises, we do not consider it appropriate to introduce a tiered model based on service size or risk.[61] Additionally, by amending the measures to clarify the explicit objective of the measures, we consider this outcomes-focused approach to be more proportionate and effective than prescribing a tiered approach.

A1.28 Therefore, we do not intend to introduce a tiered model as we consider a clear, single threshold is more proportionate and practical at this time.

Time requirements

A1.29 Several stakeholders called for clearer and faster timeframes for activating, operating, and ending crisis protocols. Demos suggested service providers must respond within eight hours and cited research showing that harmful content peaks in the first hours of a crisis.[62] Stakeholders also recommended stronger governance and specific enforcement benchmarks, such as indicators and risk assessments to adjust severity levels, and set takedown time limits for certain harms.[63]

A1.30 One stakeholder requested clarity on the expected timeframe for providers to respond to a crisis.[64]

Our response

A1.31 We note stakeholders' suggestions for fixed timelines, but our position remains that providers should activate the responsive elements of their crisis response protocol, i.e., their crisis response team and the relevant systems and processes as soon as reasonably practicable once a crisis is determined to be occurring or likely to occur on their service. At this stage, we do not consider it appropriate to set a universal time baseline, as there is insufficient evidence to support a single standard suitable for all services. Providers are therefore responsible for setting their own response and end-times, guided by their crisis indicators and risk assessments.

A1.32 How quickly a provider can implement their crisis response protocol will vary between services, as crises may unfold at different rates across services. Providers remain

[61] See paragraphs 3.82 -3.86 in the section titled 'Size of service' in Chapter 3.
[62] Demos response to the June 2025 Consultation, p.16.
[63] BILETA response to the June 2025 Consultation, p.43; Demos response to the June 2025 Consultation, pp.15-16; Full Fact response to the June 2025 Consultation, p.15; [✂].
[64] Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.16.

responsible for determining an appropriate response point within their own systems, informed by the crisis indicators and their risk assessments. Chapter 3 paragraphs 3.21-3.34 provide expanded examples for identifying and responding to a crisis, as well as conducting a post-crisis analysis. This is intended to support providers in ensuring timely and appropriate activation of their crisis response protocols.

A1.33 However, we acknowledge the evidence outlined by Demos that content spikes in the first few hours of a crisis.[65] Therefore, we have clarified explicitly that providers should activate the responsive elements of their crisis response protocol as soon as reasonably practicable once they determine that a crisis is occurring or is likely to occur on their service(s). This clarification is outlined in Chapter 3 paragraph 3.11 of the section titled 'Our decision'.

A1.34 Providers remain responsible for determining an appropriate timeframe to respond within their own systems, informed by the crisis indicators and their risk assessments.

A1.35 Our definition of a crisis remains unchanged.

Threshold for ending a crisis

A1.36 One stakeholder raised that there should be a set threshold for services to identify when a crisis has ended.[66]

Our response

A1.37 We recommend that a crisis be treated as an acute, short-term event. For this reason, a crisis response protocol should not remain active after a crisis has ended or for more than 90 days, whichever comes first. In respect of criterion for the end of a crisis, a crisis will have ended for the purpose of the measures when the criteria for determining that a crisis is occurring or is likely to occur are no longer met.

A1.38 Situations that continue for more than 90 days require a different approach. In these scenarios, services should continue to address the relevant harm but should shift their focus towards strengthening organisational resilience and longer-term planning (such as adapting 'business as usual' procedures) rather than continuing their crisis response protocols for more than 90 days.

A1.39 By the 90-day point, services should have adjusted to the 'new normal', with operations stabilised and sufficiently equipped to respond effectively to the prevailing conditions.

Stronger transparency and accountability measures

A1.40 Some civil society and government stakeholders suggested additions to the measures around stronger transparency and accountability, including but not limited to, moderation or assessment mechanisms, notification of protocols being triggered, mandatory post-crisis submissions, detailed decision logs, and disclosure of partnerships to build public trust.[67]

---

[65] Demos, 2025. Researching the riots: An evaluation of the efficacy of community notes during the 2024 Southport riots. [accessed 19 May 2026]; Institute for Strategic Dialogue, 2024. From rumours to riots: How online misinformation fuelled violence in the aftermath of the Southport attack. [accessed 19 May 2026].

[66] Molly Rose Foundation response to the June 2025 Consultation, p.18.

[67] Ofcom's Advisory Council for Northern Ireland response to the June 2025 Consultation, p.4; Antisemitism Policy Trust response to the June 2025 Consultation, p.2; Barnardo's response to the June 2025 Consultation, pp.21-22; Demos response to the June 2025 Consultation, pp.19, 21, 23, 30; Department of Justice for Northern Ireland response to the June 2025 Consultation, p.16; Full Fact response to the June 2025 Consultation, pp.9-10, 14-16; [✂]; Online Safety Act Network response to the June 2025 Consultation, p.29.

A1.41 One individual stakeholder said pre-written holding statements allowed quick responses and control of the narrative. They referred to best practices from presspage.com recommending issuing a statement within 15 minutes of a crisis to show transparency and responsiveness.[68]

Our response

A1.42 In response to concerns about transparency and evaluation, we have expanded our examples of what services could include in their post-crisis analysis.[69] This additional detail is intended to support providers in producing meaningful reflections on how their crisis response operated in practice. At the same time, we have deliberately maintained flexibility around the format and content of these analyses. Services differ widely in size, resources, and the nature of the risks they face. A flexible approach allows providers to focus on insights that are genuinely valuable for improving future responses, rather than meeting prescriptive reporting requirements that may not be proportionate or applicable for all.

A1.43 We have also considered suggestions that services should be required to routinely submit their post-crisis analyses to Ofcom or publish them publicly. We are not recommending such a requirement. The primary purpose of a post-crisis analysis is for services to learn from the incident and strengthen their internal processes. These analyses may also contain commercially sensitive or confidential information, making routine publication unlikely to be appropriate. Requiring all providers to submit their analyses would create significant regulatory and operational burdens, and we consider that resources would be better directed toward targeted engagement where the circumstances justify closer scrutiny.

A1.44 We also note that services wishing to publish their post-crisis analyses may do so, including information about how they have gathered relevant insights during the incident. While publication is not required, we recognise that some providers may see value in doing so to support transparency and public trust.

A1.45 Where necessary, Ofcom can obtain post-crisis analyses. This approach enables Ofcom to intervene when there is a clear need, without imposing blanket reporting obligations on all services. For providers with whom we do not already have an established supervisory relationship, mandatory submissions would introduce additional complexity, which we do not consider proportionate.

A1.46 Our supervisory powers play an important role in ensuring effective oversight during and after a crisis. Where appropriate, Ofcom can contact relevant services to understand whether they have activated their crisis response protocols and how they are managing emerging risks. This provides a mechanism for accountability without imposing universal reporting duties.[70]

A1.47 We recognise the importance of human oversight, transparency, and user redress. The crisis response measures do not require providers to rely solely on automation, nor to lower usual safety procedures.

---

[68] Turner, B. response to the June 2025 Additional Safety Measures Consultation, pp 71-72.
[69] See paragraph 3.34 in Chapter 3.
[70] Additionally, under section 175 of the Act, the Secretary of State may direct Ofcom to issue a public statement notice requiring a specific service provider, or providers generally, to make a publicly available statement about the steps they are taking in response to a threat to public safety or national security.

Including other bodies and agencies in the measures

A1.48 Some civil society stakeholders suggested including other public bodies (in addition to law enforcement) as part of the crisis response measure.[71] They said this might include civil society partners, local authority services and independent fact-checkers, who could support with mitigating wider harms that arise in a crisis.

A1.49 Full Fact said fact-checkers need real-time access to back-end data from service providers to identify and prioritise harmful content and understand misinformation spread, warning that lack of data hampers timely responses as seen in the 2024 riots.[72]

A1.50 Full Fact stated that Community Notes cannot replace independent fact-checking, citing evidence from Demos which it said showed how the feature was slow and invisible during the 2024 riots. Full Fact recommended the protocol require pre-crisis reviews of such tools and integration with professional fact-checking and crisis protocols.

Our response

A1.51 We recognise the important role that civil society organisations and other relevant partners can play in strengthening crisis response. Therefore, we encourage providers to, where relevant, collaborate with the relevant organisations to inform their response.

A1.52 We have considered suggestions to include a wider range of agencies and/or organisations within the measures, but do not consider this proportionate or practical at this time. Expanding formal contact obligations across multiple bodies would impose significant operational and cost burdens on providers (and those bodies) and duplicate the established role of law enforcement, which is best placed to coordinate action/response among relevant public agencies when needed.

A1.53 In our statutory report on researchers' access to information from online services, published in July 2025, Ofcom acknowledged the importance of data access for researchers working on online safety-related matters.[73] Our report, which was informed by valuable input from stakeholders, flagged researchers' reported need for real-time data access and access to internal data from services. The report also highlighted the challenges researchers face when attempting to access data for their work, and the fact that researchers from civil society, for-profit, and under-resourced organisations report particular difficulties. The report was shared with the Secretary of State for Science, Innovation and Technology, and laid before UK Parliament in summer 2025. The Government has indicated that Ofcom's report will provide an evidence base to inform the design of any future access framework supporting research into online safety matters. In parallel to our work, the UK Parliament has enacted the Data (Use and Access) Act 2025 that allows the UK Government to create, if it chooses to do so, a new framework to enable researchers to access data regarding online safety matters held by regulated services.

---

[71] Ofcom's Advisory Council for Northern Ireland response to the June 2025 Consultation, p.5; Demos response to the June 2025 Consultation, pp.17-18, 33; Full Fact response to the June 2025 Consultation, pp. 11-12; International Justice Mission response to the June 2025 Consultation, p.22; [✂];Tech Against Terrorism response to the June 2025 Consultation, p.14.

[72] Full Fact response to the June 2025 Consultation, p.13.

[73] Ofcom. Researchers' access to information from regulated online services.

Cross-service collaboration

A1.54 Several civil society stakeholders recommended cross-service provider collaboration, coordination and response during crises.[74]

Our response

A1.55 We acknowledge stakeholders' views that information-sharing across services can be valuable during crises, particularly given that illegal content and/or content harmful to children may spread quickly across multiple services. Existing voluntary industry initiatives, such as the Global Internet Forum to Counter Terrorism (GIFCT) and other sector-led collaborations, demonstrate that cross-service cooperation can support faster identification of emerging threats and more consistent mitigation approaches across the wider ecosystem.

A1.56 Providers remain free to participate in voluntary partnerships where they consider this appropriate and proportionate, but it is not a recommended component of these measures.

A1.57 Ofcom is not best placed to act as the central body responsible for coordinating information-sharing frameworks or cross-service operational structures. Establishing and running such a framework would require real-time access to services' internal data, involve substantial privacy and data-protection risks, and raise concerns around sharing commercially sensitive or competitively valuable information.

A1.58 Instead, we encourage good practices for crisis communication planning such as establishing clear internal escalation routes for high-risk content, preparing rapid response communication plans for relevant operational teams, and developing streamlined processes for sharing time-sensitive information with law enforcement or government where appropriate. Such planning can help services respond quickly and consistently during a crisis.

A1.59 Our approach towards cross-service collaboration remains unchanged.

Responses related to law enforcement

A1.60 A range of stakeholders stressed the need for clear guidance and safeguards on law enforcement channels, including due process and privacy, and called for dedicated, well-staffed crisis communication channels with rapid response and strict limits on use.[75]

Our response

A1.61 We have clarified that the dedicated law enforcement communication channel applies only to large services and is intended solely for use during crises and for law enforcement to share information with services on crisis-related matters. It is not intended to replace or shortcut established legal processes for routine requests for data or information. Providers

[74] Full Fact response to the June 2025 Consultation, pp.7-8; Molly Rose Foundation response to the June 2025 Consultation, p.18; Online Safety Act Network response to the June 2025 Consultation, p.29; Tech Against Terrorism response to the June 2025 Consultation, p.14.

[75] Ofcom's Advisory Council for Northern Ireland response to the June 2025 Consultation, pp.3-4; Commissioner Designate for Victims of Crime Northern Ireland response to the June 2025 Consultation, p.8; Full Fact response to the June 2025 Consultation, p.18; Gender and Tech Research Lab response to the June 2025 Consultation, p.2; [✂]; Microsoft response to the June 2025 Consultation, p.11; NPCC response to the June 2025 Consultation, pp.16-17; [✂]; [✂]; Pinterest response to the June 2025 Consultation, p.6.

and other relevant agencies must continue to rely on the existing due-process mechanisms that govern law enforcement and other data requests.

A1.62 As stated in Chapter 3, we expect the channel to facilitate time-sensitive communication relevant to a crisis

A1.63 Decisions on retention periods, preservation, and the handling of relevant material must be agreed directly between services and law enforcement under existing legal frameworks. The scope of these measures is tied to providers' duties under the Act. Ofcom has no general power to require providers to disclose material to law enforcement, except where explicitly set out in the Act, such as provisions relating to child sexual abuse material (CSAM).

A1.64 We do not consider it proportionate to extend the requirement for a dedicated law enforcement communication channel to smaller high-risk services. Expanding the measures in this way would require law enforcement to manage potentially hundreds of new communication lines, creating significant operational pressures and resource demands. For smaller services, establishing and maintaining such channels would also be a substantial burden. Our assessment is that the requirement is best targeted at large services, where the scale and speed of content dissemination create the greatest need for rapid coordination with law enforcement.

Evidence on the link between online content and offline violence

A1.65 A number of stakeholders stated that the link between online content and real-world offline violence is unclear.[76]

Our response

A1.66 We acknowledge points raised that the measures assume a relationship between online content and offline harms. However, our assessment and the design of the measures is based on evidence showing that during crises, certain types of illegal content and/or content harmful to children can increase and spread, thereby heightening both online and offline risks. Moreover, in such circumstances there can be a risk of the services being used themselves in the commission or facilitation of offences.

A1.67 Research shows that offline trigger events are often followed by increases in online hate, abuse, harassment, threats and violent material, including calls for violence and the sharing of violent imagery.[77] There is also evidence that terrorist content can surge during crises, and in some contexts these spikes have been linked to increased offline risk.[78]

A1.68 Our definition of a crisis, therefore, does not assume that online content automatically causes offline harms. It reflects evidence that certain online harms intensify during crises

[76] Demos response to the June 2025 Consultation, p.28; Francis, S. response to the June 2025 Consultation, p.14; [✂]; [✂];Name Withheld 26 response to the June 2025 Consultation, p.11; Name Withheld 27 response to the June 2025 Consultation, p.12; Porter, J. response to the June 2025 Consultation, pp.8-9.

[77] Faloppa, F., Gambacorta, A., Odekerken, R., van der Noordaa, R., 2023. Study on preventing and combating hate speech in times of crisis. Council of Europe. [accessed 28 April 2026]; Gill, A., 2024. Mosque explosion call woman jailed for online post, BBC, 14 August. [accessed 28 April 2026]

[78] Conway, M., Scrivens, R., and Macnair, L., 2019. Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends. The International Centre for Counter-Terrorism – The Hague 10, 1–24 [accessed 28 April 2026].

and can contribute to environments where risks escalate rapidly, posing a wider threat to public safety. As a result, the crisis response measures are developed to help services manage those risks appropriately, in line with their safety duties under the Act.

Boosting reliable information

A1.69 A number of civil society respondents recommended that we include a measure to boost reliable information during crises and to help users to understand which information is reliable.[79]

Our response

A1.70 We recognise the importance of users being able to access reliable and accurate information during times of crisis, including information from authorised public bodies and trusted local figures. Access to clear, trustworthy updates can help users navigate periods of uncertainty and better understand fast-moving events. We therefore acknowledge the value that official sources, local leaders, and other credible voices can play in supporting public understanding during crises.

A1.71 Transmission Critical, our most recent Public Service Media Review, highlighted the importance of trusted and accurate news – and in particular public service broadcaster (PSB) news – for providing critical information that holds institutions to account and supports civil society and the democratic process. [80]

A1.72 We also work to support people to access reliable and accurate information through our media literacy work. Our media literacy strategy is anchored in the Communications Act 2003 with the duty to promote media literacy. The Online Safety Act introduced some new media literacy objectives including duties to focus on content of democratic importance and misinformation and disinformation. In addition, under the Online Safety Act, Ofcom is required to publish a statement recommending ways in which services might develop, pursue and evaluate activities or initiatives relevant to media literacy. Our Media Literacy Statement of Recommendations supports access to reliable and accurate information by setting out steps services can take to help people navigate and thrive in a rapidly evolving digital landscape. Our recommendations to services include encouraging online services to provide meaningful context around content (including through labels, metadata and other indicators) and to work with expert third parties to direct users toward high-quality, trustworthy information when it matters most. Collectively, these expectations aim to strengthen users' critical engagement skills and support a more informed and resilient public.

A1.73 Ofcom also commissions work in communities to develop media literacy skills amongst population groups. For example, our Informed Voices project supports young people, particularly first-time voters, in navigating online mis and disinformation relating to elections. We have worked with Parent Zone and community and youth organisations to deliver online campaigns and in person skills building activities in Wales and Scotland ahead of Senedd and Scottish parliament elections.

---

[79] Demos response to the June 2025 Consultation, pp.20, 35; Digital Resilience in Education (Welsh Government) response to the June 2025 Consultation, p.16; Full Fact response to the June 2025 Consultation, pp.6-7, 13-14; Online Safety Act Network response to the June 2025 Consultation, p.29; [✂].
[80] Ofcom. Transmission critical.

Misinformation

A1.74 Full Fact noted that misinformation can be lawful, and that the false communication offence does not cover those unaware that their content is false or without intent to harm. It noted the limitations of the Act to address misinformation and called for clear, transparent protocols to tackle misinformation linked to serious incidents.[81]

Our response

A1.75 We acknowledge Full Fact's evidence on misinformation during the 2024 summer riots and its call for clearer incident protocols, but the crisis response measures operate within the scope of the Act and we can only make recommendations which are sufficiently linked to providers' duties under the Act.

A1.76 Within this remit, we encourage services to maintain clear governance and transparent processes, record key decisions in post-crisis analysis, and, where appropriate, work voluntarily with independent fact-checkers or other expert bodies.

Clarification of evidence

A1.77 The Free Speech Union disputed the accuracy of a piece of evidence cited by Ofcom in our June 2025 Consultation. The piece of evidence was regarding Ofcom's reference to the conviction of an individual for a false communications offence, which we discussed in relation to our crisis response measures. The Free Speech Union clarified that this was inaccurate, and that the individual in question was never convicted of a crime.[82]

Our response

A1.78 The Free Speech Union is correct – while the individual had been arrested for a false communications offence, she was later released without charge. We apologise for this inaccurate reference.

A1.79 This inaccuracy was in relation to only one of the pieces of evidence on which the measures are founded and therefore we maintain our position on the increased instances of harm during crises, with further evidence supporting our view set out in Chapter 3: 'Crisis Response'.

Small services

A1.80 We received a range of feedback regarding small services. This feedback included providing further guidance to small services and highlighted that the measures must be proportionate for smaller services, given their limited resources and distinct roles during crises.[83]

Our response

A1.81 We have included non-exhaustive examples of crisis indicators, systems and processes, and information in a post-crisis analysis in paragraphs 3.21-3.34 Chapter 3: 'Crisis Response'. This is intended to support all services in understanding the types of actions that may be

[81] Full Fact response to the June 2025 Consultation, p.5.
[82] Free Speech Union response to the June 2025 Consultation, p.2.
[83] ACT – The App Association response to the June 2025 Consultation, p.11; Check My Ads response to the June 2025 Consultation, p.14; Demos response to the June 2025 Consultation, p.30; International Justice Mission response to the June 2025 Consultation, p.21; [✂]; [✂]; [✂].

proportionate and effective during a crisis. Our assessment is that providing this additional information offers clarity while ensuring that obligations remain achievable for services with varying levels of capacity.

A1.82 We note stakeholder views that smaller services may be more vulnerable to exploitation due to more limited moderation and safety capabilities. Our measures are intended to apply in a proportionate and scalable way, taking into account the size and risk profile of a service. We expect providers, including smaller services where relevant risks arise, to consider how their crisis response arrangements can be adapted to their operational capacity while remaining effective.

A1.83 We note stakeholder views on the important role that smaller services can play in supporting communities during crises, and their concern that additional moderation could detract from this function. Our measures focus specifically on providers' responses to the relevant content and do not affect lawful speech or routine community interactions. On this basis, we consider that smaller services will continue to operate as vital community spaces.

A1.84 We agree that our measures must work for smaller services in scope. We have provided additional information in Chapter 3 to help all services, especially resource-limited providers to identify indicators, conduct a comprehensive post-crisis analysis and execute a crisis response suited to their capabilities, recognising that illegal content and/or content harmful to children may originate on smaller services. We agree that reliable digital infrastructure support small and medium-sized enterprises, but such policy matters sit outside the scope of these measures.

A1.85 We acknowledge that crisis-related content can spread across services and that dynamics between very large and smaller services may affect amplification. While we cannot mandate advertising-market remedies, we encourage providers to coordinate internally where relevant and to consider voluntary and proportionate steps to limit monetisation of violating content during crisis periods.

Best practices

A1.86 Individual and civil society stakeholders highlighted best practices for crisis response, proposing a broad mix of best practices, including:

- Systematic safety by design approach to crisis protocols, including testing and scenario planning.[84]
- The importance of clear communication policies as part of crisis protocols and suggested these should be mandated.[85]
- The need for crisis protocols to reflect local contexts, including language needs, cultural sensitivities, and region-specific patterns of disorder.[86]

[84] Barnardo's response to the June 2025 Consultation, p.21; BILETA response to the June 2025 Consultation, p.40, 43; Demos response to the June 2025 Consultation, p.32; Full Fact response to the June 2025 Consultation, pp.9-11, 20; Kira, B. (Dr) response to the June 2025 Consultation, pp.12-15; [✂].

[85] Demos response to the June 2025 Consultation, pp.20, 34; [✂].

[86] Ofcom's Advisory Council for Northern Ireland response to the June 2025 Consultation, pp.1-2, pp.4-5; Commissioner Designate for Victims of Crime Northern Ireland response to the June 2025 Consultation, p.8.

- Clearer governance structures, including defined roles, decision-making processes, accountability, and communication arrangements, aligned with recognised command frameworks.[87]
- Recommending further moderation measures.[88]

Our response

Safety by design

A1.87 We agree with stakeholders that safety by design is an essential part of online safety.

A1.88 The term 'safety by design' can be interpreted in various ways, but for the purpose of this statement we use it to mean a proactive approach to integrating safety considerations into the design cycle of products, systems, or processes. This includes making iterative improvements to existing systems or longstanding services or features. It also can include retirement (replacing or removing a feature or functionality altogether), as well as ensuring new services or features are designed with safety in mind from the outset.

A1.89 We consider that many features of these measures promote safety by design by recommending baseline actions to protect users in the event of a crisis.

A1.90 An essential element of safety by design is iterating to address and anticipate risks presented by different features and functionalities of online services, hence our iterative approach; from setting up indicators to monitoring for a crisis to conducting a post-crisis analysis.

A1.91 We note the importance of including preventative measures before escalation and stabilisation after an incident. While the crisis response measures focus on actions during a defined crisis period, providers may find value in aligning their internal processes with broader resilience frameworks, including pre-crisis preparation and post-incident risk assessment. This flexibility allows services to build on the measures in ways that suit their operating models while remaining consistent with their duties under the Act.

A1.92 We consider that the stages set out in the crisis response measures reflect the full lifecycle of a crisis. If providers wish to adopt additional preventative and post-crisis practices, we encourage them to explore and implement these where they consider them appropriate for their service.

A1.93 We recognise the value of ensuring that crisis response protocols remain effective over time, and we encourage services to test their protocols periodically where this is relevant. Such testing can help verify that internal processes function as intended and support preparedness in the rare event of a crisis. Where providers find it useful, they may draw on existing testing and exercising frameworks, such as those used in broader emergency planning, to inform how they conduct these activities.

Crisis communication

A1.94 We recognise the value of implementing effective crisis-communication practices and encourage service providers to implement them where relevant. See paragraph A1.58 in the cross-service collaboration section for more details.

---

[87] Full Fact response to the June 2025 Consultation, pp.10, 15, 16.
[88] Name Withheld 4 response to the June 2025 Consultation, p.11; NPCC response to the June 2025 Consultation, p.17; SWGfL response to the June 2025 Consultation, p.23.

A1.95 We recognise that some providers may find it helpful to issue a short public statement soon after identifying a crisis. We also acknowledge the importance of protecting online communities during crises, particularly those who may be more vulnerable or at greater risk of harm, and we encourage providers to take appropriate steps to safeguard the communities on their services during such periods.

A1.96 We acknowledge stakeholder views on the potential value of pre-prepared holding statements in facilitating timely and transparent communication during crises. Providers may incorporate this practice into their own procedures where it aligns with their service design and operational capacity.

Moderation

A1.97 We agree that transparent communication and clear routes for users to challenge moderation decisions can support trust, including during crises. Services remain responsible for ensuring that their moderation processes – whether human-led, automated, or hybrid – are effective and in compliance with their existing duties under the Act. We also recognise that smaller providers may need to adopt approaches suited to their scale, and this is reflected in the flexible design of the measures.

A1.98 We note the examples provided regarding community-driven moderation approaches. Service providers may adopt such models where appropriate, where doing so could support the effective operation of their crisis response protocols.

A1.99 Though we acknowledge the evidence that certain technologies can be effective in limiting the spread of non-consensual intimate images (NCII), we are not addressing NCII through these measures.[89] And while the crisis response measures do not recommend specific technologies or moderation techniques, providers may choose to adopt tools where appropriate, lawful and proportionate.

A1.100 We acknowledge concerns about AI systems that may be misused to generate or distribute illegal content. However, the crisis response measures are focused on strengthening providers' crisis response and we do not intend to include recommendations on technical measures at this time.

A1.101 We recognise the systemic risks associated with offender behaviour shifting to encrypted environments and the emergence of hyper-realistic AI-generated illegal content. These are important concerns, and providers must take proportionate steps under their existing duties to mitigate such harms. However, the crisis response measures themselves do not recommend specific technologies as this would not be appropriate across all services. Providers remain responsible for selecting appropriate tools and approaches that are lawful, effective, and suited to their risk profile.

Local context

A1.102 We recognise that understanding local context is important for effective moderation, and our measures on resourcing moderation are designed to help address the particular needs of services' United Kingdom user base in relation to languages.[90] Where a provider identifies gaps in contextual understanding that affect how certain harms are identified or assessed, they should take steps to remedy these through appropriate training or

[89] Our June 2026 Statement on Detecting Intimate Image Abuse.
[90] See ICU C6 Illegal Content user-to-user Codes and PCU C6 of the Protection of Children user-to-user Code.

guidance. This is reflected in our broader content moderation measures in the Illegal Content and Protection of Children user-to-user Codes of Practice (user-to-user Codes).[91]

A1.103 We recognise stakeholder observations regarding the formation of online communities during crises and the associated risks, including coordinated inauthentic behaviour and exploitation by perpetrators. Where relevant, we encourage providers to take these dynamics into account when designing and operating their crisis response protocols.

A1.104 Regarding working with local organisations, see our response in paragraphs A1.51-A1.53 on working with civil society organisations and other relevant partners during a crisis.

Governance

A1.105 We consider that our clarification to the post-crisis analysis requirement – specifically, setting out the expectation that providers record key decisions taken during a crisis – will help ensure that important governance decisions are captured throughout the crisis response period. We also recognise that, in some cases, an initial debrief shortly after a crisis has ended may be useful for providers to reflect on welfare, risks, and immediate lessons learned. We encourage providers to carry this out where relevant to their operations.

Existing practice

A1.106 The Online Safety Act Network noted our reference to evidence that some providers have crisis mechanisms but said it was unclear if we had assessed their effectiveness or used them as a baseline for best practice. It said this was an oversight and argued we should have provided additional requirements based on available evidence.[92]

Our response

A1.107 In developing our measures, we drew on the available evidence regarding existing crisis mechanisms across the industry, existing government practice, and relevant academic evidence. Our goal was to develop the measures considering current industry practices, while allowing flexibility for providers to design protocols that are appropriate and proportionate to their services.

A1.108 We acknowledge the view that further requirements could be derived from existing evidence. However, we assess that it is appropriate to set out principles-based expectations rather than prescriptive requirements.

Costs

Assessment of costs and cost drivers

A1.109 One industry stakeholder and one civil society stakeholder said that they agreed with our assessment of impacts and costs.[93]

A1.110 Another industry stakeholder agreed that the time required to design, operate, and analyse the protocol would be the main source of costs.[94]

---

[91] See Chapter 2 of Volume 2: Service Design and User Choice in the December 2024 Statement on Protecting People from Illegal Harms, and Section 14 of Volume 4: What should services do to mitigate the risks of online harms to children in the April 2025 Statement on Protecting Children from Harms Online.
[92] Online Safety Act Network response to the June 2025 Consultation, p.30.
[93] Check My Ads response to the June 2025 Consultation, p.15; [✂].
[94] Pinterest response to the June 2025 Consultation, p.6.

A1.111 One civil society stakeholder agreed that the factors we set out would cause costs to vary between services, while another highlighted that implementation of the measures may need to scale with resources and size.[95]

Our response

A1.112 We note the agreement with our assessment of costs and the factors causing costs to vary.

Cost of preparing a crisis response protocol

A1.113 One industry stakeholder said that our cost analysis for preparing crisis response protocols appeared arbitrary.[96]

Our response

A1.114 We consider that we have based our assessment of costs for this element on reasonable assumptions as to how long the development of a protocol would take, and we have not received evidence to suggest alternative assumptions would be more appropriate.

Cost of a crisis response team

A1.115 One stakeholder said that our assumption of a crisis response team made up of 5 to 10 reallocated staff plus one senior leader would be too small for many services, citing evidence given by large social media service to a select committee that it used over 100 staff during the 2024 summer riots.[97]

Our response

A1.116 We consider that 5 to 10 staff in a crisis response team is a reasonable assumption for a core team for the basis of our impact assessment. However, we acknowledge that there will in addition be content moderators who many need to be reallocated to focus on this work, as noted in our consultation. We have assumed that these content moderators would not need significant additional training (though they will likely need to be guided by the crisis response team), and therefore this does not pose an additional cost for services. While this shift of employee time is an opportunity cost for the service, we consider that this is proportionate to the benefits to increasing content moderators focusing on the crisis, and in any case, content would need to be moderated in accordance with existing content moderation measures.

Reallocation of content moderators during a crisis

A1.117 One industry stakeholder said that it had implemented a crisis management protocol that reallocates moderation resource.[98]

A1.118 One stakeholder said we should allow providers flexibility to assign resources and not require reallocation of content moderators.[99]

---

[95] Evangelical Alliance response to the June 2025 Consultation, p.14; Full Fact response to the June 2025 Consultation, p.20.
[96] Google response to the June 2025 Consultation, p.36.
[97] Full Fact response to the June 2025 Consultation, p.20 (citing Science, Innovation and Technology Committee, 25 February 2025. Oral evidence: Social media, misinformation and harmful algorithms, HC 44, p.3).
[98] Snap Inc. response to the June 2025 Consultation, p.19.
[99] Google response to the June 2025 Consultation, p.36.

Our response

A1.119 We consider that the measures provide services flexibility in how to resource their crisis response. We have made an assumption that this will likely be delivered through redeploying existing moderation resource to focus on the crisis however providers can choose how to manage this to meet their safety duties.

Necessary experience

A1.120 One stakeholder said that our proposals were unworkable because they assumed service providers had corporate expertise and significant resources, which was not the case for many providers.[100]

Our response

A1.121 We consider that services need to have or develop sufficient in-house expertise to address crises on their service. In Chapter 3 paragraphs 3.21-3.34 we provide expanded examples on identifying and responding to a crisis, as well as conducting a post-crisis analysis, which should support smaller providers in undertaking these activities. We also note that there may be third-party trust and safety providers that could be incentivised to develop crisis response protocols that could be affordable for smaller providers and provide access to external expertise.

Proportionality assessment

A1.122 Several stakeholders challenged our impact assessment, saying that we have placed too much emphasis on keeping costs low and should have weighed the financial costs to providers against societal harms caused by illegal content.[101]

Our response

A1.123 We have considered the benefits of the measures, as set out in the section titled 'Effectiveness and benefits' in Chapter 3: 'Crisis response'. We are recommending the measures because we consider that it would help protect individuals in the event of a crisis. We have considered costs to service providers as part of our duties under the Act that the measures must be proportionate in the section titled 'Costs and Impacts' in Chapter 3: 'Crisis response'.

Freedom of expression

A1.124 Several stakeholders expressed concerns that the measures would have adverse impacts on freedom of expression.[102] Some were of the view that the proposed measures, particularly when involving automated moderation, would result in censorship or could result in the suppression of important information, journalism, and civic reporting. Other stakeholders considered that the measures would result in the restriction of lawful content and were of the view that this was disproportionate and irrational.

---

[100] Klaushofer, A. response to the June 2025 Consultation, p.1.

[101] BILETA response to the June 2025 Consultation, p.44; Full Fact response to the June 2025 Consultation, p.20.

[102] [✂]; [✂]; Francis, S. response to the June 2025 Consultation, p.16; Free Speech Union response to the June 2025 Consultation, p.1, p.4; [✂]; [✂]; Microsoft response to the June 2025 Consultation, p.11; Name Withheld 26 response to the June 2025 Consultation, p.12; Porter, J. response to the June 2025 Consultation, p.11; [✂]; Together Campaign response to the June 2025 Consultation, p.6; [✂].

A1.125 One stakeholder suggested that providers should be required to implement a fast review and restore approach to protect lawful speech, including political and journalistic content.[103]

A1.126 One stakeholder was of the view that our concept of a crisis event went beyond legislative requirements and could lead to overzealous responses.[104]

Our response

A1.127 As set out in our June 2025 Consultation, the measures do not recommend that service providers adopt a differential approach to content moderation in the event of a crisis. The measures are focussed on providers' processes and procedures and are designed to assist providers in being prepared for crisis situations and responding effectively to them should they arise.

A1.128 We acknowledge that there is a risk that providers adopt a crisis response protocol which prioritises over accuracy in respect of content moderation during a crisis. However, we reiterate that this is not recommended in the measures (see Chapter 3 paragraph 3.75). As noted in our June 2025 Consultation, the impact of this risk on users' rights to freedom of expression (to the extent that it materialises) must be balanced against the very significant public interest in moderation of relevant content during a crisis.

A1.129 We do not consider it appropriate or proportionate to recommend that providers adopt a differential approach to content moderation during a crisis. Furthermore, existing measures are in place in relation to appeals and the time it takes to deal with them, and the crisis response measures do not change these.[105]

A1.130 We do not agree with the view that our concept of a crisis event goes beyond legislative requirements. We consider that the measures are rooted in providers' existing duties under the Act on illegal content and content which is harmful to children and therefore are within the scope of the Act. We reiterate that the measures are focussed on addressing the impact of illegal content and/or content harmful to children. This is made clear in our definition of a crisis, which requires a relationship between the event and illegal content and/or content harmful to children.

A1.131 In our June 2025 Consultation we also noted that there were existing safeguards in place to minimise the risk of interference with the right to freedom of expression. We explained that providers have incentives to limit the number of false positives that occur through content moderation, to meet user expectations and to minimise the costs of dealing with appeals. In addition, we noted that existing measures on accuracy of decision making and appeals also act as a safeguard for freedom of expression and that furthermore, the Illegal Content Judgements Guidance (ICJG) and the Guidance on Content Harmful to Children were prepared with careful consideration of the right to freedom of expression. Providers are encouraged to consult this guidance when implementing the measures to help them correctly identify when freedom of expression considerations are particularly relevant to certain content.

---

[103] Name Withheld 26 response to the June 2026 Consultation, p.12.
[104] Free Speech Union response to the June 2025 Consultation, p.3.
[105] For example, ICU D8 recommends that large and/or multi risk providers set performance targets for dealing with appeals relating to time and accuracy and should take certain matters into account when prioritising appeals, including whether the decision was taken by proactive technology, past error rates, and the seriousness of the action taken against the user.

A1.132 Additionally, in accordance with the principles of the Act and our duties under the Human Rights Act 1998, we will have regard to the importance of freedom of expression and association, and the right to privacy, when making any decisions about enforcement in relation to these measures. This acts as a further safeguard for these rights.

Human rights impact assessments

A1.133 A stakeholder suggested that Ofcom should require providers to carry out human rights impact assessments when implementing the measures.[106]

A1.134 Some stakeholders considered that terms such as 'harm' and 'hate' are subjective, and that a lack of legal clarity would enable abuse of the measures and censorship.[107]

Our response

A1.135 We do not consider this is necessary or proportionate, taking account of providers' duties under section 22 of the Act. Section 22 of the Act imposes a duty upon all user-to-user services to have regard to the importance of protecting users' rights to freedom of expression when deciding on and implementing safety measures and policies and imposes an additional duty on category 1 services to carry out impact assessments relating to freedom of expression and privacy rights. Such impact assessments must include consideration of the impact on news publishers and journalistic content.

A1.136 The terms 'harm' and 'hate' are defined by the Act and the existing user-to-user Codes, and the measures were drafted by reference to the meaning of those terms under the Act and the user-to-user Codes. For the avoidance of doubt, reference to 'harm'/'harmful' for the purpose of these measures means an illegal harm or a type of content which is harmful to children, and 'hate' means content amounting to one of the priority offences defined in the Schedules to the Act, which fall under the "threats, abuse, and harassment (including hate)" illegal harm, or hate offences under content harmful to children. As noted in paragraph A1.131, we have also provided the ICJG and the Guidance on Content Harmful to Children to help providers make these judgements.

Personal data and privacy risks

A1.137 BILETA, an individual respondent, and the Information Commissioner's Office (ICO) raised concerns about privacy and data protection risks when crisis response protocols are implemented, particularly if a provider adopts a crisis response protocol which prioritises speed of content moderation over accuracy.[108]

Our response

A1.138 Any crisis response protocol implemented by providers must continue to comply with existing data protection and privacy regulations. This includes adhering to principles such as data minimisation, storage limitation, and ensuring that any personal or special category data processed for the purpose of identifying crisis indicators is handled lawfully. Providers are also encouraged to consider ICO guidance on content moderation, accuracy, and fairness obligations.

---

[106] Demos response to the June 2025 Consultation, p.24.
[107] Free Speech Union response to the June 2025 Consultation, pp.2-3; Name Withheld 27 response to the June 2025 Consultation, pp.13-14.; Together Campaign response to the June 2025 Consultation, p.5.
[108] BILETA response to the June 2025 Consultation, pp.42, 44; [✂]; Information Commissioner's Office (ICO) response to the June 2025 Consultation, p.31.

A1.139 The crisis response measures do not recommend or require providers to prioritise speed over accuracy in their moderation processes. For more information on rights and freedom of expression see paragraphs 3.63-3.71 in Chapter 3.

A1.140 For providers choosing to adopt novel technologies, including AI systems, as part of their crisis response protocols, we encourage adherence to existing best-practice frameworks. These may include conducting appropriate risk and bias assessments, using privacy-preserving technologies where feasible, and ensuring robust oversight of automated systems.

Flexibility of the measures

A1.141 A number of stakeholders commented on the importance of flexibility in implementing the measures. Their points included perceived burden of requirements, use of existing practices and the appropriateness of the measure to certain services.[109]

- Google recommended that we should explicitly allow providers to have a combined crisis response plan covering illegal harms and content harmful to children, rather than requiring two separate plans.[110]
- One individual stakeholder said our proposals overlooked key best practices that prioritise proportionality, privacy, and service diversity. [111] They highlighted community-driven moderation models used by Reddit and Wikipedia during crises, citing examples from the 2020 US Capitol riot.
- Pinterest cautioned against overly prescriptive process requirements and said providers should be able to tailor governance and documentation to their structure, size, and risk profile to avoid unnecessary burden. [112]

Our response

A1.142 We note concerns about administrative burden and agree that the crisis response protocols must remain proportionate and effective. The measures are deliberately flexible, and providers may rely on existing incident frameworks rather than creating parallel systems. We do not expect this flexibility to create undue administration or reduce effectiveness. Instead, it is intended to avoid a one-size-fits-all approach that could be counter-productive. We also reiterate that the post-crisis analysis is primarily a learning tool for providers, helping them refine what works on their service.

A1.143 We note that risk profiles vary across services. The measures are risk-based and allows providers to tailor their crisis protocol to their operations. These measures support timely escalation to large services by law enforcement during crises.

A1.144 We do not intend to introduce more prescriptive recommendations at this stage. Our intention is to maintain flexibility so that services of different types and sizes can develop approaches suited to their specific risks and operational capabilities. This flexibility also enables us to learn as the crisis-response landscape evolves and as more evidence becomes available about what is effective in practice. Over time, and as we gain a clearer

[109] Google response to the June 2025 Consultation, p.36; [✂], [✂]; NPCC response to the June 2025 Consultation, p.16; Online Safety Act Network response to the June 2025 Consultation, p.29; [✂]; Pinterest response to the June 2025 Consultation, p.6.
[110] Google response to the June 2025 Consultation, p.36.
[111] [✂].
[112] Pinterest response to the June 2025 Consultation, p.6.

understanding of industry behaviour and outcomes during crises, we may consider whether greater specificity or additional requirements would be appropriate.

A1.145 We have developed the measures so that services can choose the most appropriate crisis indicators for their size, functions, and risk profile.

A1.146 Providers may implement a single, combined crisis response protocol that covers both illegal content and content harmful to children, rather than maintaining two separate plans.

Consideration of the impacts on advertisers during crises

A1.147 Check My Ads Institute argued digital advertising benefits from viral content and recommended requiring very large online platforms (VLOPs) to disclose monetisation revenues and refund advertisers where possible.[113]

Our response

A1.148 We recognise that advertising incentives can interact with virality during crises. However, the crisis response measures are focused on providers' duties to manage illegal content and content harmful to children. Providers may, where proportionate, choose to deploy ad-integrity measures as part of their protocols, but the measures do not recommend specific monetisation practices.

A1.149 We agree that reliable digital infrastructure support small and medium-sized enterprises, but such policy matters sit outside the scope of these measures.

A1.150 We recognise the importance of human oversight, transparency, and user redress. The crisis response measures do not require providers to rely solely on automation, nor to lower due-process standards.

A1.151 We note that risk profiles vary across services. The measures are risk-based and allows providers to tailor their crisis protocol to their operations.

[113] Check My Ads response to the June 2025 Consultation, p.14.

A2. Legal Framework

A2.1 In this annex we set out the statutory basis of Ofcom's role and the issues we must consider when preparing Codes.

A2.2 We also discuss our approach to proposing a new measure in the Codes and the impact assessment of the measure in the Codes.

The Online Safety Act 2023 and the Codes of Practice

A2.3 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. Section 12 of the Act also places duties on providers of regulated services likely to be accessed by children to take steps to prevent and protect children from encountering content harmful to children.

A2.4 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.

A2.5 The safety duties in the Act only apply to the design, operation and use of services in the UK.[114] They also apply to the design, operation and use of a service as it affects UK users (duties that relate to users).[115] The 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.[116]

A2.6 In December 2024,[117] and April 2025,[118] 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.

A2.7 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 (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.

A2.8 Under the Act, we are required to prepare and issue the following sets of Codes for user-to-user and search service providers (for example, 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 (CSEA) content (relating to the offences set out in Schedule 6); and

[114] This is defined in section 4 of the Online Safety Act 2023 (the Act).
[115] Section 8(3) of the Act.
[116] Schedule 4 to the Act, paragraph 11.
[117] Ofcom. Protecting People from Illegal Harms Online.
[118] Ofcom. Protecting Children from Harms Online.

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).

A2.9 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.

A2.10 We are committed to further strengthening these Codes to protect all users. We have therefore decided in this statement to amend both the Illegal Content and Protection of Children user-to-user Codes.

Ofcom's duties and online safety functions

A2.11 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

A2.12 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.

A2.13 As a public authority, Ofcom must act lawfully, rationally and fairly.

A2.14 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.[119]

A2.15 In performing that principal duty, the 2003 Act sets out that Ofcom's regulatory activities must be transparent, accountable, proportionate, consistent and targeted only at cases where action is needed.[120] We must also 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.

A2.16 The 2003 Act further requires[121] that Ofcom must have regard to several factors, as they appear to us to be relevant in the circumstances,[122] and as a result we have carefully considered the following in making our decisions:

[119] Section 3(1) of the Communications Act 2003 (2003 Act).
[120] We must also have regard to any other principles appearing to us to represent best regulatory practice.
[121] Section 3(4A) of the 2003 Act.
[122] 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

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;
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.

A2.17 In line with our additional duties under the 2003 Act,[123] 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 specific additional Illegal Content Codes considerations

A2.18 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.[124] 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 that apply to services of various kinds and sizes must be proportionate to our assessment of the risk of harm presented by services of that kind or size.

A2.19 We must also ensure that the measures described in the Illegal Content Codes are compatible with pursuit of a 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). These are explained in more detail in Annex 3: Statutory Tests and Impact Assessments.

A2.20 Under the 2003 Act, we are also required to conduct impact assessments when preparing an amendment to a Code, including an assessment of the impact on small and micro businesses.[125]

A2.21 We consider that assessing measures based on our impact assessment criteria is the right approach to ensuring our Codes protect users from illegal content and content harmful to

---

different interests of persons in the different parts of the UK and of the different ethnic communities within the UK. See Schedule 4 tests.

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

[124] Schedule 4 of the Act.

[125] Section 7 of the 2003 Act, as amended by section 93 of the Act.

children online while also protecting their rights and enabling service providers to operate and innovate in the market. We are open to revisiting the best way to assess our measures within our obligations as the regime develops.

Human rights

A2.22 It is unlawful for Ofcom to act in a way which is incompatible with the European Convention on Human Rights (ECHR).[126]

A2.23 Of particular relevance to Ofcom's functions under the Act are the right to freedom of expression (Article 10 ECHR) and the right to privacy (Article 8 ECHR). In formulating our decisions in this Statement, we have carefully analysed the potential for interference with ECHR rights, to make sure any interference is proportionate.

A2.24 The right to freedom of expression includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authority. Article 10(2) of the ECHR states that this right may be restricted in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

A2.25 Article 8(1) of the ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8(2) sets out limited qualifications, stating that public authorities must not interfere with the exercise of this right unless necessary in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

A2.26 Other ECHR rights which may also be relevant to Ofcom's functions under the Act are the right to freedom of thought, conscience and religion (Article 9 ECHR) and the right to freedom of assembly and association (Article 11 ECHR).

A2.27 These are qualified rights, but the need for any interference with these rights must be construed strictly and established convincingly. Any interference must be prescribed by or in accordance with the law; pursue a legitimate aim and be necessary in a democratic society – in other words, it must be proportionate to the legitimate aim pursued and correspond to a pressing social need.

A2.28 In considering whether impact on these rights are proportionate, our starting point is to recognise that Parliament has determined that providers of regulated services must take proportionate measures to protect users from illegal content and, where relevant, the commission and facilitation of priority offences. We therefore start from the position that UK users should be protected from the harms set out in the Act and place weight on all the specific evidence of harm set out in our Register of Risks. A substantial public interest exists in these outcomes. Overall we have sought to strike a fair balance between securing adequate protections for users from harm (and their human rights in respect of this) and the ECHR rights of users, other interested persons (including for example, persons who host websites or who may be featured in content on regulated services or whose content might be on those services regardless of whether or not they are service users) and service providers, as relevant.

[126] Section 6 of the Human Rights Act 1998.

Equality Impact Assessment and Welsh language

A2.29 We have considered the equality impacts of the measures set out in this statement, detailing our understanding of any particular impacts on protected groups in the UK.

A2.30 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 use the Welsh language and the need to treat the Welsh language no less favourably than English (in accordance with Welsh language standards).

A2.31 We have set out our considerations on these matters in Annex 3: Statutory Tests and Impact Assessments.

The Deregulation Act 2015

A2.32 Ofcom is required, when exercising our regulatory functions, to have regard to the desirability of promoting economic growth, including through considering the importance of ensuring the regulatory action we take is necessary and proportionate.[127] This duty is referred to as the "growth duty".

A2.33 We are also required to have regard to the UK Government's statutory guidance on the growth duty.[128] 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. [129] Among other things, it also identifies particular drivers of economic growth, including innovation, investment and competition.

A2.34 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. As such, we did not expressly consider the growth duty in our June 2025 Additional Safety Measures Consultation. For this statement, we have therefore reassessed our impact assessment of these measures and the combined impact, by considering the wider economic impacts of our decision.

[127] Section 108 of the Deregulation Act 2015.
[128] Section 110(3) of the Deregulation Act 2015.
[129] Department for Business and Trade, 2024. Growth Duty: Statutory Guidance – Refresh

A3. Statutory Tests and Impact Assessments

Our approach to the Impact Assessment

A3.1 In developing our recommendations, we are required to consider the impact and proportionality of the measures on both service providers and online users.

A3.2 We assess the impact of our recommended measures based on the following factors:

a) the prevalence and impact of the harm the measures are combatting;
b) the efficacy of the measures in combatting relevant harms (and, by extension, the benefits the measures would deliver);
c) the direct and indirect costs of the measures;
d) the impact the measures would have on privacy and freedom of expression; and
e) any risks associated with the measures.

A3.3 We also consider the proportionality of applying the measures to either all, or specific subsets, of service providers. This remains consistent with our approach to impact assessments in the December 2024 and April 2025 Statements.

A3.4 Our assessment took into consideration the anticipated impacts, costs, and benefits of the measures over and above those which are expected to arise from existing measures.

A3.5 In our combined impact assessment we have considered the costs and benefits of the recommended measures set out in this statement alongside the existing measures as an overall package.

A3.6 The detailed impact assessment, including the combined assessment, is set out in Chapter 3 of this statement.

Equality Impact Assessment

A3.7 We are also required to consider the impact of our recommendations on individuals and communities with protected characteristics. This is called an Equality Impact Assessment (EIA).

A3.8 We conduct the EIAs in accordance with Ofcom's legal obligations under:

a) Section 3 of the Communications Act 2003

   i) To further the interests of citizens in relation to communications matters; and
   ii) secure the adequate protection of citizens from harm presented by content on regulated services.

b) section 149 of the Equality Act 2010, requiring public authorities to have due regard to the need to:

   i) eliminate unlawful discrimination, harassment and victimisation;
   ii) advance equality of opportunity; and
   iii) foster good relations between different groups.

c) section 75 of the Northern Ireland Act 1998, which extends these obligations to include political opinion, marital status, and dependants

A3.9 We did not receive stakeholder comments on our EIA related to these measures.

A3.10 In preparing this statement, we have carefully considered the potential impacts of our measures on people sharing protected characteristics (including age, sex, race, disability, religion or belief, sexual orientation, gender reassignment, pregnancy and maternity, and marriage and civil partnership, as well as dependants and political opinion in Northern Ireland). 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.

A3.11 The measures described in this statement are designed to reduce the risk of the following priority illegal harms: terrorism, hate, harassment, stalking, threats and abuse, and foreign interference. They are also designed to address the following types of priority content harmful to children: abusive content, content inciting hatred, violent content (instructions for an act of serious violence against a person), violent content (person). They include stronger protections against the risks arising from a significant increase in relevant illegal content and relevant content harmful to children and, where relevant, the increased risk that a service will be used to commit or facilitate a priority offence, during a crisis. We consider our measures will have positive impacts for people with protected characteristics, particularly those belonging to minority ethnic and religious groups that may be subjected to increased levels of online hate and abuse during crises.

A3.12 We have considered whether the measures could have negative impacts on equality of opportunity or the fostering of good relations. We do not consider that there will be any such impacts; the measures should ensure that providers are prepared for crises and respond in a timely and effective manner.

Welsh Language Impact Assessment

A3.13 The Welsh language has official status in Wales. To give effect to this, certain public bodies, including Ofcom, are required to comply with the Welsh Language Standards.[130] Accordingly, we have considered:

- the potential impact of our policy proposals on opportunities for persons to use the Welsh language;
- the potential impact of our policy proposals on treating the Welsh language no less favourably than the English language; and
- how our proposals could be formulated to have or increase a positive impact, or not to have adverse effects or to decrease any adverse effects.

A3.14 We did not receive stakeholder comments on our Welsh Language Impact Assessment related to these measures.

A3.15 Ofcom's powers and duties in relation to online safety regulation are set out in the Act and must be exercised in accordance with our general duties under section 3 of the Communications Act 2003. 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.

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

We have not identified any likely negative impacts on the Welsh language arising from our decision to introduce these measures.

Statutory tests

A3.16 In designing the Codes, the Act requires us to have regard to a number of principles and objectives, set out in Schedule 4 to the Act. The Communications Act 2003 also places a number of duties on Ofcom in carrying out our functions, including requiring us to have regard to the risk of harm to citizens presented by content on regulated services.

A3.17 In Chapter 3 of this statement, we set out our final recommended measures for service providers. We consider that our recommended measures meet the requirements set out in Schedule 4 to the Act and section 3 of the Communications Act 2003. In this section, we take each of the relevant requirements in turn and briefly set out how we have met them in reaching our recommended measures.

Duties and principles

The Communications Act 2003

> Section 3(1): It shall be the principal duty of Ofcom, in carrying out their functions: 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.

A3.18 We have set out in this statement how the recommended measures will mitigate the risks of illegal harm to all users, and the risks of harm to children, thereby furthering their interests as well as the interests of citizens in the UK more generally.

A3.19 We have considered the interests of consumers in relevant markets (particularly users of regulated services) as part of our assessment of the proportionality of our recommendations, including any potential impacts on the provision of services to users.

A3.20 We have also considered the rights of users and other interested persons in our rights assessment for each measure, where we consider any impacts of the measure on users' rights (children's and adults' as relevant), including their rights to freedom of expression and privacy, as required by the Online Safety Act.

> Section 3(3): In performing their duties under subsection (1), Ofcom must have regard in all cases to (a) the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed, and (b) any other principles appearing to Ofcom to represent best regulatory practice.

A3.21 In the interest of transparency, accountability and fairness (and as required by the Online Safety Act) we consulted stakeholders and have set out the evidence and reasoning informing our decision. Chapter 3 of this statement includes impact assessments for the measures we have decided to recommend.

A3.22 At paragraphs A3.1-A3.6 we have explained how we approach impact assessments. Our impact assessment of the measures considers effectiveness, costs, rights and explained why we consider the measures are proportionate to the benefits to children and adults.

See our impact assessment guidance for more information on how we approach impact assessments.[131]

A3.23 Our measures are informed by our assessment of the risks posed by illegal content to all users and the risks of harm to children. We have prioritised developing measures that can effectively mitigate the significant risks identified in our analysis and those required by the Act and have targeted the measures at the types of illegal content and content harmful to children we consider are most likely to pose a risk during crises, and at the kinds of services that are at the most risk of these types of illegal content and content harmful to children because this would lead to the greatest benefits given the risks posed.

Section 3(2)(g): In carrying out our functions, Ofcom are required to secure the adequate protection of citizens from harm presented by content on regulated services, through the appropriate use by providers of such services of systems and processes designed to reduce the risk of such harm.

A3.24 The changes we are making to our Codes of Practice will mitigate the risks to users from illegal content, and the risks to children from content harmful to them, by ensuring that providers are prepared to address the risk of an increase in such content on their services during a crisis, and the risk that their services will be used to commit or facilitate a priority offence.

A3.25 The measures are informed by our own assessment of the risks of harm, as set out in our Illegal Harms and Children's Register of Risks and Risk Profiles.[132] [133] They are also informed by additional sources as detailed in our assessment of effectiveness and benefits. We explain in Chapter 3, from paragraph 3.35 how the measures will be effective in reducing risk and harm.

A3.26 In relation to matters to which section 3(2)(g) in the 2003 Act is relevant, section 3(4A) sets out that in performing their duties under subsection (1), Ofcom must have regard to such of the following as appear to them to be relevant in the circumstances:

(a) The risk of harm to citizens presented by content on regulated services.

A3.27 Our Illegal Harms and Children's Register of Risks and Risk Profiles set out the risks of harm posed by content on regulated services. These risks, alongside findings from services' risk assessments, largely inform what measures will be appropriate for a service provider to address the risk of harm to citizens. The measures included in the Codes vary across services based on their risk and size. In Chapter 3, from paragraph 3.35 we discuss the risk of harm that we are seeking to address and why we consider our measures will be effective.

A3.28 The Guidance on Content Harmful to Children sets out examples of content, or kinds of content, that we consider to be, or consider not to be, primary priority content and priority content that is harmful to children. The guidance is intended to support providers of Part 3 services that are likely to be accessed by children in making judgements about whether

[131] Ofcom. Ofcom's approach to impact assessment.
[132] Ofcom. Illegal Harms Register of Risks; Ofcom. Protection of Children's Register of Risks.
[133] Ofcom. Children's Risk Assessment Guidance and Risk Profiles; Ofcom. Illegal Harms Risk Assessment Guidance

content on their service is content that is harmful to children as defined in the Online Safety Act.[134]

(b) The need for a higher level of protection for children than for adults.

A3.29 Our Codes already ensure a higher level of protection for children than for adults, and we consider that they will continue to do so with the addition of these measures.

(c) The need for it to be clear to providers of regulated services how they may comply with their duties set out under the Act.

A3.30 Our measures, and the explanation in this document of how the measures work, aim to provide clarity and tangible steps that services can take to meet their duties in the Online Safety Act.

A3.31 We have issued various guidance in the past that will support providers in complying with the measures that we are recommending (for example, the Illegal Content Judgements Guidance and Guidance on Content Harmful to Children).[135]

A3.32 We have explained in Chapter 2, paragraph 2.2 that services which choose to implement the measures in the Codes will be considered as complying with relevant duties. We have also explained that service providers may seek to comply with their safety duties by choosing to take alternative measures.

(d) The need to exercise their functions so as to secure that providers of regulated services may comply with such duties by taking measures, or using measures, systems or processes, which are (where relevant) proportionate to (i) the size or capacity of the provider in question, and (ii) the level of risk of harm presented by the service in question, and the severity of the potential harm.

A3.33 The Risk Assessment Guidance and Children's Risk Assessment Guidance take account of the nature and size of services, for example in recommending what evidence providers should take into consideration to support their risk assessments.[136]

A3.34 We have clearly identified in the measures the types, sizes and risk profiles of services we recommend adopt each measure, for the reasons given in Chapter 3, from paragraph 3.76. The Online Safety Act requires us to ensure measures are proportionate, and we recognise that the size, capacity, and risks of services differ widely. We therefore do not take a one-size-fits-all approach. Instead, we have set out what types of service we think should use specific safety measures to comply with their duties, with the most extensive expectations placed on the riskiest services.

(e) and (f) The desirability of promoting the use by providers of regulated services of technologies which are designed to reduce the risk of harm to citizens presented by content on regulated services; and the extent to which providers demonstrate, in a way that is transparent and accountable, that they are complying with their duties.

[134] Ofcom. Guidance on Content Harmful to Children.
[135] Ofcom. Guidance on Content Harmful to Children; Ofcom. Illegal Content Judgements Guidance.
[136] Ofcom. Children's Risk Assessment Guidance and Profiles; Ofcom. Risk Assessment Guidance and Risk Profiles.

A3.35 While providers may choose to use a variety of technologies designed to reduce the risk of harm, these measures do not specifically recommend the use of such technologies.

A3.36 Section (4) of the 2003 Act sets out other matters to which we must have regard in performing our duties, to the extent they appear to us relevant in the circumstances.[137]

> Section 3(4) : Ofcom must also have regard, in performing those duties, to such of the following as appear to them to be relevant in the circumstances […] (b) the desirability of promoting competition in relevant markets, (d) the desirability of encouraging investment and innovation in relevant markets; (h) the vulnerability of children and of others whose circumstances appear to Ofcom to put them in need of special protection; (i) the needs of persons with disabilities, of the elderly and of those on low incomes; (j) the desirability of preventing crime and disorder; (k) the opinions of consumers in relevant markets and of members of the public generally; (l) and the different interests of persons in the different parts of the United Kingdom, of the different ethnic communities within the United Kingdom and of persons living in rural and urban areas.

A3.37 In recommending these measures we have had regard to the desirability of promoting competition and encouraging investment and innovation. Our measures provide flexibility for services to decide how to achieve compliance. As set out in Chapter 3, section titled impact and costs, we have considered the interests of consumers in relevant markets as part of our impact assessments of proposed measures, including any indirect impacts on consumers in cases where our measures could affect competition, investment and innovation in respect of the online services they use. To the extent that the measures relate to illegal content safety duties, these aim to prevent crime and disorder. In relation to the opinions of consumers in relevant markets and of members of the public generally we have taken account of stakeholder responses to our consultation on these measures and to previous consultations.

A3.38 In recommending measures in pursuit of children's safety duties, we have had regard to the objective of a higher standard of protection for children than for adults, assessing whether measures are expected to be effective at achieving this.

A3.39 In our Equality Impact Assessments, we have considered the needs of persons with protected and listed characteristics. We have also considered our Welsh language obligations. See Annex 3, from paragraph A3.7-A3.15.

Schedule 4 of the Online Safety Act 2023

A3.40 As required by paragraph 1 of Schedule 4 to the Act, we have considered the appropriateness of provisions of these additional measures for the Codes to different kinds and sizes of Part 3 services and the providers of differing sizes and capacities and we have set out our reasons for recommending the application of the measures to the services we have recommended they apply to in Chapter 3, section titled 'Who these measures apply to.'

A3.41 We have had regard to the principles in Schedule 4 to the Act, as follows:

> Paragraph 2(a): providers of Part 3 services must be able to understand which provisions of the code of practice apply in relation to a particular service they provide.

[137] Section 4, Communications Act 2003

A3.42 We have clearly identified the types and sizes of service that the measures apply to, as set out in our draft amended Codes and explained further in in Chapter 3, section titled 'Who these measures apply to.'

Paragraph 2(b): the measures described in the code of practice must be sufficiently clear, and at a sufficiently detailed level, that providers understand what those measures entail in practice.

A3.43 Having regard to the need for it to be clear to providers of regulated services how they may comply with their duties, we have aimed to be as clear as possible and to include an appropriate level of detail in the June 2025 Consultation, this statement, and the amended Codes. We have sought to be sufficiently detailed and precise while ensuring our measures are technically feasible and proportionate for the range of services in scope of the Act and these measures. Our approach to the amended Codes strikes the balance between providing certainty about what providers need to do and allowing them flexibility to implement the measures in a way that works in the context of their own service and is proportionate. While we recognise that some aspects of the measures are not prescriptive, we have explained why this is not possible.

Paragraph 2(c): the measures described in the code of practice must be proportionate and technically feasible: measures that are proportionate or technically feasible for providers of a certain size or capacity, or for services of a certain kind or size, may not be proportionate or technically feasible for providers of a different size or capacity or for services of a different kind or size;

A3.44 As noted in in Chapter 3, section titled 'Who these measures apply to.', we have clearly identified what types and sizes of services the measures apply to. We have considered proportionality and technical feasibility as part of our assessment of impacts across this statement.

A3.45 We have taken into account evidence of current practice by user-to-user service providers who are already taking steps that are similar or related to measures that we recommend. We consider effectiveness, costs, rights impacts, and other relevant factors in our assessment of proportionality.

Paragraph 2(d): the measures described in the code of practice that apply in relation to Part 3 services of various kinds and sizes must be proportionate to Ofcom's assessment under section 98 of the risk of harm presented by services of that kind or size.

A3.46 We have identified the relevant risks of harm that the measures address and explained why we consider the measures are proportionate in the light of those harms. As required by section 3(4A)(b)(ii) of the 2003 Act, in considering proportionality we have had regard to the severity of the potential harm as well as the level of risk of harm, as identified in the Illegal Harms and Children's Register of Risks. We have clearly identified the types and sizes of services the measures will apply to, for the reasons given in in Chapter 3, section titled 'Who these measures apply to.'.

A3.47 Overall, the Codes place more demanding expectations on services that pose greater risks. Having regard to the desirability of encouraging investment and innovation in the markets for regulated services and these technologies, our recommendations provide sufficient flexibility for services. Our impact assessment for the measures, as well as our combined

impact assessment, also take into account the cost to services as we acknowledge additional costs can affect investment and innovation.

Ofcom's Online Safety Objectives

User-to-user services

A3.48 As required by paragraph 3 of Schedule 4 to the Act, we have ensured that our measures are compatible with the pursuit of the applicable online safety objectives for user-to-user services as set out in this sub-section.

A3.49 In line with paragraph 11 of Schedule 4 to the Act, these measures relate only to the design or operation of a Part 3 service (a) in the United Kingdom, or (b) as it affects United Kingdom users of the service.

Paragraph 4(a)(i): a service should be designed and operated in such a way that the systems and processes for regulatory compliance and risk management are effective and proportionate to the kind and size of service.

A3.50 The Codes already include measures related to governance and accountability, and we are not changing these.

Paragraph 4(a)(ii): a service should be designed and operated in such a way that the systems and processes are appropriate to deal with the number of users of the service and its user base.

A3.51 In our December 2024 Statement (paragraph 14.14) and our April 2025 Statement (paragraph 21.53) we said that content moderation, automated content moderation, and reporting and complaints measures in our existing Codes were set having regard for (among other things) the number of users of a service and its user base. We consider these additional measures to be compatible with this objective.

Paragraph 4(a)(iii): a service should be designed and operated in such a way that United Kingdom users (including children) are made aware of, and can understand, the terms of service.

A3.52 Our existing Codes recommend measures related to terms of service. We are not amending these or introducing additional related measures.

Paragraph 4(a)(iv): a service should be designed and operated in such a way that there are adequate systems and processes to support United Kingdom users.

A3.53 Our existing Codes recommend measures relating to reporting and complaints. These additional measures do not amend these or introduce additional reporting and complaints related measures.

Paragraph 4(a)(vi): a service should be designed and operated in such a way that the service provides a higher standard of protection for children than for adults.

A3.54 A number of existing measures are compatible with this objective. For example, the user reporting and complaints measures (ICU D2 and PCU D2) recommend that systems and processes should be easy to access and easy to find, helping child users report content harmful to children to the service provider. These additional measures are also compatible with this objective and are designed to ensure that providers are prepared to address the

risk of an increase in certain types of content harmful to children on their service in the event of a crisis.

Paragraph 4(a)(vii): a service should be designed and operated in such a way that the different needs of children at ages are taken into account.

A3.55 In the December 2024 Statement (Chapter 10: 'Terms of Service' and Chapter 8: 'User-to-User Settings, Functionalities, and User Support', we set out how we had regard to the different needs of children at different ages. In the April 2025 Statement, we noted that service providers have a duty, as part of their children's risk assessment, to assess their user base, including separate consideration to children in different age groups on the service and assessing how the design and use of the service affects the level of risk of harm to children and that we therefore consider that this objective will be secured in particular via the children's risk assessment duties and the Children's Risk Assessment Guidance.

Paragraph 4(a)(viii): a service should be designed and operated in such a way that there are adequate controls over access to the service by adults.

A3.56 The existing Illegal Content Codes include a measure to limit the access of proscribed organisations. In the December 2024 Statement we set out why we do not consider it appropriate to restrict access to services generally by adults. These additional measures do not recommend any changes to controls over access to services by adults.

Paragraph 4(a)(ix): a service should be designed and operated in such a way that there are adequate controls over access to, and use of, the service by children, taking into account use of the service by, and impact on, children in different age groups.

A3.57 In the April 2025 Statement we explained how our age assurance measures take into account the use of the service by, and impact on, children in different age groups. In relation to our content moderation measures and recommender systems measures, we also explained that providers should consider children's ages as a factor when designing the part of their system relating to the appropriate action. These additional measures do not recommend any changes to controls over access to, and use of, the service by children.

Paragraph 4(b): a service should be designed and operated so as to protect individuals in the United Kingdom who are users of the service from harm, including with regard to:

algorithms used by the service,

functionalities of the service, and

other features relating to the operation of the service.

A3.58 Our existing Codes recommend measures related to recommender systems. These additional measures do not amend these or introduce additional reporting and complaints related measures

A3.59 We have consulted on recommending measures relating to recommender systems and live streaming, and our decisions in relation to these measures will be published in Autumn 2026.

A3.60 We have not at this stage consulting on recommending measures relating to paragraph 4(a)(v) – "(in the case of a Category 1 service) users are offered features to increase their control over certain categories of content that they encounter and the users they interact

with" – given it is specific to Category 1 services only. We will explore proposed measures for categorised services in greater detail in Phase 3 of our work.

A3.61 We consider these additional measures are consistent with this objective.

Other duties

A3.62 Under section 92(2) of the Act, Ofcom must have regard to the Secretary of State's statement of strategic priorities for online safety when carrying out online safety functions. We have had regard to this statement, which was designated on 2 July 2025, shortly after we published our June 2025 Consultation. We responded to the statement on 25 July 2025[138] and have taken into account in finalising our decisions set out in this statement.

[138] Ofcom. Letter to Government on the Statement of Strategic Priorities for Online Safety.

A4. Further detail on economic assumptions and analysis

A4.1 This annex provides further information related to the economic analysis used to support our decision on the crisis response measures assessed in this statement.

A4.2 We have made some general cost assumptions which are set out here. These general assumptions are combined with assumptions specific to these measures that are set out in the section titled 'Costs and impacts' in Chapter 3.

Labour costs

A4.3 We used data from the Annual Survey of Hours and Earnings (ASHE), to develop our estimates for the labour cost required to implement the code measures. All quantified estimates of costs are provided in 2025 prices, unless otherwise stated, which is the most recent data available.[139] Our June 2025 Additional Safety Measures Consultation (June 2025 Consultation) used 2024 prices which was the most recently available data at that time.[140]

A4.4 We used the ASHE 2025 gross median earnings for the following Standard Occupational Classification (SOC) 2020 references: [141]

- Programmers and software development professionals' salary (2134) to estimate the cost of 'software engineer' time used when developing our cost estimates.
- Database administrators and web content technicians' salary (3133) to estimate the cost of 'content moderator' time when developing our cost estimates.[142]
- Professional Occupations salary (2) to cover a range of professions that are employed at various online services and might be required to implement code measures.[143] This could be legal employees, operations, product managers and so forth.

[139] Office for National Statistics (ONS), 2025. Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14. Data from 2025 is provisional at time of writing. [accessed 11 May 2026]
[140] Our December 2024 Statement on Protecting People from Illegal Harms (December 2024 Statement) and our April 2025 Statement on Protecting Children from Harms Online (April 2025 Statement) used 2023 prices.
[141] We note that in our June 2025 Consultation annex we stated that we had used the "gross median *full-time* earnings" – however, this was not correct. We used gross medium earnings "for all employee jobs" in our estimates and the salary figures presented in the Annex.
[142] We note that in our June 2025 Consultation annex the salary code was wrongly reported as 3113, not 3133. This four-digit SOC 2020 code (unit group code 3133) includes occupations such as content, chat, web and website moderators as well as other occupations such as database administrators and web content. technicians.
[143] We note that in our June 2025 Consultation annex we stated that we had used the "Business, median and public service professionals (24)" salary – however, this was not correct. We used the "Professional Occupations (2)" salary in our estimates and the salary figures presented in the Annex. This is also what was used in our cost estimates for our December 2024 Statement and April 2025 Statement.

A4.5 We chose these occupations because they are likely to develop and/or manage the systems and processes that in-scope service providers will need to have to comply with the regime.[144]

A4.6 For some service providers median UK wage rates may differ from actual salary rates.

a) This may be especially the case for larger service providers based in the US, who may have higher salary levels. The salary costs of some types of staff, such as software engineers with certain specialisms, may vary and may be considerably higher in some cases. To take account of this, we have calculated a higher salary estimate, which is double the value of our lower estimate.
b) Conversely, some service providers may outsource some relevant work to locations where average pay is lower than the UK, which may reduce costs. To the extent this is the case, our salary range may tend to overstate costs.

A4.7 We applied a 22% uplift to the gross wage costs to account for non-wage labour costs, such as employers' National Insurance contributions.[145] This is calculated based on the most recent 2024 Blue Book data. Estimates in our June 2025 Consultation used a 21% uplift based on 2023 data, which was the most recent data at the time of that publication.

A4.8 Table A5.1 shows the 'low' and 'high' labour cost estimates for different time periods, including the 22% uplift, for each of the three occupations. The figures are based on annual labour costs, and we have calculated the monthly, weekly and daily estimates.[146]

Table A4.1: Low and high range – Estimates of labour costs

Occupation	Low	High
	Annual labour cost estimates	
Software engineer	£67,816	£135,632
Content moderator	£43,938	£87,877
Professional occupations	£55,210	£110,420
	Monthly labour cost estimates	

[144] Annual Survey of Hours and Earnings (ASHE) documentation does not explicitly state that gross salaries include bonuses, but our understanding is that the gross pay includes bonuses, tips and other payments.
[145] ONS, 2021. *Uplifts from wages and salaries to total employment costs: a note on data*. [accessed 11 May 2026]. ONS recommends dividing the 'employer's social contributions (D.12)' by 'wages and salaries (D.11)' to arrive at the uplift. Both series are published as part of the annual UK National Accounts: Blue Book time series. They provide economy wide estimates of D.11 and D.12 annually. At time of writing, the most recent data available is for 2024.
[146] When producing cost estimates for the measure, we have used resourcing estimates based on different time periods (e.g. days/weeks/months) suitable for the particular measure. The annual wages are derived from the ONS, 2025 Earnings and hours worked, occupation by four-digit SOCs, Table 14.7a. [accessed 11 May 2026]. Gross median annual pay for all employee jobs, 2025 provisional estimates. Monthly, weekly and daily wages are all derived from this annual figure. The monthly wages are derived from dividing the annual wages by the number of months in a year (12). The weekly wages are derived by dividing the annual figure by 45.54 (the number of working weeks per year, calculated by dividing the number of working days by the number of working days in a week). The daily wages are derived from dividing the annual wages by the number of working days in a year. We assume on average there are 228 working days in a year. This assumes people work five days a week and that there are eight bank holidays and on average people take an additional 25 days leave a year.

Software engineer	£5,651	£11,303
Content moderator	£3,662	£7,323
Professional occupations	£4,601	£9,202
	Weekly labour cost estimates	
Software engineer	£1,489	£2,978
Content moderator	£965	£1,930
Professional occupations	£1,212	£2,425
	Daily labour cost estimates	
Software engineer	£298	£596
Content moderator	£193	£386
Professional occupations	£242	£485

Source: ONS (2025), Annual Survey of Hours and Earnings. Includes 22% uplift. Calculations are performed based on the underlying median gross salary (the 'low' estimate, before uplift is applied) and then uplifted by 22%.

A4.9 For the measures that require input from senior management, we have used salary estimates from additional occupations. These include senior managers and senior leaders with an estimates annual labour cost of £122,000 to £183,000.[147]

Non-engineering costs for system changes

A4.10 Where system or other software changes associated with a measure involve a software cost, we typically match the amount of engineering time with an equivalent amount of non-engineering time for work carried out by people in professional occupations. This is to account for labour time that a business might need to spend on a system change, for instance, legal or project management.

Maintenance costs for system changes

A4.11 Where system or other software changes associated with a measure involve an initial cost, we have assumed an ongoing annual maintenance cost of 25% of the initial cost. These ongoing costs reflect work likely required to ensure the system continues to operate as intended. We have applied this assumption in the absence of actual information about the ongoing maintenance costs. This is consistent with the approach we took in the December 2024 Statement on Protecting People from Illegal Harms Online and the April 2025 Statement on Protecting Children from Harms Online.

[147] This is based on simple assumptions we have made of £100,000 salary for a senior manager and £150,000 for a senior leader, which are then uplifted by the 22% for non-wage labour costs.

A5. Glossary

A5.1 This glossary sets out definitions of terms used throughout the statement.

Terms	Definition
Abuse and hate content (Content harmful to children)	Content, described in section 62(2) of the Act, which is abusive and which targets any of the following characteristics— (a) race, (b) religion, (c) sex, (d) sexual orientation, (e) disability, or (f) gender reassignment and/or content, described in section 62(3) of the Act, which incites hatred against people— (a) of a particular race, religion, sex or sexual orientation, (b) who have a disability, or (c) who have the characteristic of gender reassignment.
Our April 2025 Statement on Protecting Children from Harms Online (April 2025 Statement)	*'Protecting children from harms online'*, published by Ofcom on 24 April 2025, available at Statement: Protecting children from harms online.
Child	A person under the age of 18.
Child user	A user under the age of 18.
Children's Access Assessments Guidance	Guidance for Part 3 services on children's access assessments, available at Children's access assessments.
Protection of Children's Register of Risks	The assessment of the risks of harm to children from content harmful to children on user-to-user and search services that Ofcom is required to prepare under section 98 of the Act, available at Children's Register of Risks
Children's Risk Assessment	The most recent children's risk assessment, identifying and assessing the risk of harm to individuals from illegal content and content harmful to children, carried out by the provider, pursuant to sections 11 and 28 of the Act.
Children's Risk Profiles	Prepared under section 98 of the Act and as set out in Part 3 of the Children's Risk Assessment Guidance
Children's safety duties	The safety duties protecting children in sections 12 and 29 of the Act.
Codes of practice (Codes)	The set of measures recommended for compliance with the illegal content safety duties, children's safety duties, and reporting and complaints duties that Ofcom is required to prepare under section 41 of the Act.

Terms	Definition
Content	Anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description.[148]
Crisis	A crisis is an extraordinary situation in which there is a serious threat to public safety in the United Kingdom either: as a result of a significant increase in specified kinds of illegal and/or harmful content on the service; and/or which has caused or is highly likely to cause a significant increase in specified kinds of illegal and/or harmful content on the service.
Our December 2024 Statement on Protecting People from Illegal Harms (December 2024 Statement)	*'Protecting people from illegal harms online'*, published by Ofcom on 16 December 2024, available at Statement: Protecting people from illegal harms online.
Digital Services Act	Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC.
EA 2010	The Equality Act 2010.
ECHR	The European Convention on Human Rights (incorporated into domestic law by the Human Rights Act 1998).
Foreign Interference Offence (FIO)	An offence under section 13 of the National Security Act 2023 (foreign interference).
Fraud and financial services offences	A number of offences relating to fraud and financial services, such as but not limited to fraud by abuse of position, participating in fraudulent business, or the contravention of the prohibition on carrying on regulated activity unless authorised or exempt.[149]
Generative artificial intelligence (GenAI)	AI models that can create text, images, audio and videos, typically in response to a user prompt.
Guidance on Content Harmful to Children	The guidance which gives examples of content that Ofcom considers to be (or not to be) PPC and PC that is harmful to children that Ofcom is required to produce undersection 53 of the Act. The guidance is available at Guidance on Content Harmful to Children.

[148] Section 236 of the Act.
[149] An offence under: sections 2, 4, 7, or 9 of the Fraud Act 2006; section 49(3) of the Criminal Justice and Licensing (Scotland) Act 2010; sections 23, 24, or 25 of the Financial Services and Markets Act 2000; sections 89 or 90 of the Financial Services Act 2012.

Terms	Definition
Harassment, stalking, threats, and abuse (Illegal content)	A range of offences such as, but not limited to, threats to kill, causing harassment, alarm or distress, causing fear of violence, and stalking.[150]
Harm	Means physical or psychological harm. References to harm presented by content, and any other reference to harm in relation to content, have the same meaning given to it by section 234 of the Act.
Hate offences (Illegal content)	Public order offences relating to stirring up hatred on the grounds of certain protected characteristics.[151]
Illegal content	Content that amounts to a relevant offence.
Illegal content judgement guidance (ICJG)	The guidance about making illegal content judgements that Ofcom is required to produce under section 193 of the Act. It is available at Illegal Content Judgement Guidance.
Illegal content safety duties	The duties in section 10 of the Act (U2U services).
Illegal harm	Harms arising from illegal content and the commission and facilitation of priority offences.
Intimate image abuse	An offence of sharing or threatening to share intimate images or film.
Large service	A service with more than 7 million monthly active UK users.
Moderation	When a service provider reviews and assesses content to determine whether it is harmful to children or not, or whether it is in breach of the terms of service or publicly available statement of the service, and takes appropriate action based on that determination We use 'content moderation' when referring to U2U services.
Priority content	A category of content that is harmful to children, as defined in section 62 of the Act.[152]
Priority illegal content	Content which amounts to a priority offence.

[150] An offence under: section 16 of the Offences against the Person Act 1861; sections 4, 4A, or 5 of the Public Order Act 1986; sections 2, 2A, 4, or 4A of the Protection from Harassment Act 1997; article 4s or 6 of the Protection from Harassment (Northern Ireland) Order 1997 (S.I. 1997/1180 (N.I. 9)); sections 38 or 39 of the Criminal Justice and Licensing (Scotland) Act 2010 (asp 13).

[151] An offence under: sections 18, 19, 21, 29B, 29C, or 29E of the Public Order Act 1986; sections 31 or 32 of the Crime and Disorder Act 1998; section 50A of the Criminal Law (Consolidation) (Scotland) Act 1995.

[152] We have typically grouped the different kinds of priority content as follows: abuse and hate content, bullying content, violent content, harmful substances content, dangerous stunts and challenges content. This reflects the definition in section 62 of the Act.

Terms	Definition
Priority offences	The offences set out in Schedules 5 (terrorism offences), 6 (CSEA offences) and 7 (priority offences) to the Act.
Record keeping and review guidance	The guidance that Ofcom is required to produce under section 52(3) of the Act to help services to comply with their record keeping and review duties under sections 23 (U2U) and 34 (search) of the Act, available at Record-Keeping and Review Guidance.
Register of Risks	The assessment of the risks of harm from illegal content on U2U and search services that Ofcom is required to prepare under section 98 of the Act, available at Register of Risks
Regulated user-generated content	User-generated content with certain exceptions, as defined in section 55(2) of the Act.
Risk assessment	The most recent risk assessment carried out by the provider pursuant to section 9 of the Act.
Risk assessment guidance	The guidance to assist services in complying with the risk assessment duties that Ofcom is required to produce under section 99 of the Act. Our Risk assessment guidance is available at Risk Assessment Guidance.
Risk factor	A characteristic associated with the risk of one or more kinds of harm.
Risk of harm	The possibility of individuals encountering harm on a Part 3 service.
Risk profiles	Prepared under section 98 of the Act and as set out in Appendix A of the Illegal Content Risk Assessment Guidance.
Service	A regulated user-to-user or search service, i.e. only the U2U or search part of the service.
Service type	A characteristic that in general refers to the nature of the service. For example, social media services and messaging services.[153]
Small service	A service which is not a large service.
Takedown duty	The duty under section 10(3)(b) of the Act for a U2U service to use proportionate systems and processes designed to swiftly take down any (priority or non-priority) illegal content when it becomes aware of it.

[153] Certain service types have been selected because our evidence suggests that they play a role in children encountering harmful content.

Terms	Definition
Terms of Service	All documents comprising the contract for use of the service (or of part of it) by United Kingdom users.
Terrorism	An offence specified in Schedule 5 to the Act, including but not limited to offences relating to proscribed organisations, encouraging terrorism, training and financing terrorism.
The Act	The Online Safety Act 2023.
U2U	Shorthand for 'user-to-user' service, which means an internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service.
User base	Users of a service. A user does not need to be registered with a service to be considered a user of that service.[154]
User-generated content	Content (a) that is: (i) generated directly on the service by a user of the service, or (ii) uploaded to or shared on the service by a user of the service, and (b) which may be encountered by another user, or other users, of the service by means of the service.
User-to-user services	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.
Violent content (content harmful to children)	Content which encourages, promotes or provides instructions for an act of serious violence against a person or animal.[155]

[154] Section 227 of the OS Act makes clear that 'it does not matter whether a person is registered to use a service' for them to be considered a 'user.'

[155] Content which— (a) depicts real or realistic serious violence against a person; (b) depicts the real or realistic serious injury of a person in graphic detail. Content which— (a) depicts real or realistic serious violence against an animal; (b) depicts the real or realistic serious injury of an animal in graphic detail; (c) realistically depicts serious violence against a fictional creature or the serious injury of a fictional creature in graphic detail. Defined by Section 62(6) and 62(7) of the Act.