Full Fact's Submission to Ofcom's Additional Safety Measures Consultation

Summary

1. Full Fact is grateful for the opportunity to provide evidence to Ofcom's consultation on Additional Safety Measures to strengthen its Codes of Practice for regulated providers of online services (referred to in this submission as 'service providers').

2. As the UK's leading independent fact checking charity, Full Fact has a longstanding interest in the effective management of serious information incidents. We have been involved in fact checking a range of incidents – including the Covid-19 pandemic and the riots in summer 2024 – to ensure that misinformation was flagged and corrected, where possible. This submission draws from our fact checking and from our policy experience, including a framework that Full Fact developed for managing information incidents ('the Framework').[1]

3. This submission focuses on Ofcom's recommendations for service providers' crisis response protocols ('the Protocol'). It highlights the problems with the underlying legislative framework that limit the effectiveness of the Protocol; explores how to develop the scope and ambition of the Protocol; ways in which the recommended systems and processes could be enhanced; and the proposed measures to tackle serious information incidents. It also includes proposals for clarifying and expanding the suggested definition of a 'crisis', and considers the effectiveness of the measures for smaller service providers and the impacts of the measures.

4. Whilst we welcome Ofcom's consultation on the Protocol, we have concerns about the scope and ambition of the proposal. In our view, it should be adapted into a broader framework for managing incidents, overseen by Ofcom, using levels of severity and involving more key stakeholders; the Protocol must not become a weaker baseline than service providers' existing systems but should instead drive up standards; and the definition of 'crisis' should be expanded, including to cover public health and national security as well as public safety.

About Full Fact

5. Full Fact fights bad information. We are a team of independent fact checkers, technologists, researchers, and policy specialists who find, expose and counter the harm it does.

6. Bad information ruins lives. It promotes hate, divides society, damages people's health and undermines democracy. We tackle it in four ways: checking claims by politicians, public institutions, in the media and online; asking people to correct the record where possible to reduce the spread of specific claims; campaigning for system changes to make bad information rarer and less harmful; and advocating for high standards in public debate.

7. Full Fact is a registered charity funded by individual donations, charitable trusts, companies and other sources. Funding information is available on our website.[2]

Recommendations

8. In light of our evidence, we make the following recommendations:

[1] Full Fact (2021) Framework for Information Incidents
[2] Full Fact (2025) Funding

Improve the underlying legislative framework

- There should be a review of the Online Safety Act 2023 ('the OSA') to determine whether it is capable of addressing the scale of harmful content circulating online, with a view to tackling the collective harms caused by misinformation, including in relation to crises.
- Pending that review, there should be an assessment of whether to include additional priority offences in the OSA, such as key offences that are harmful to elections.
- Ofcom should revisit the categories of content that are within scope of the Protocol to broaden its lens and applicability to a wider range of information incidents.

Expand the scope and ambition of the Protocol

- Ofcom should coordinate a centralised framework for information incidents and support information-sharing between – and provide guidance and advice to – service providers.
- The Protocol should be adapted into a broader framework for managing incidents with crises at the upper end, using different levels of severity and indicators.
- Service providers should be required to establish crisis communication plans, with clear lines of communication to the police, Ofcom, government agencies, the press and others.
- Service providers should notify Ofcom, and make it clear to their users, when they initiate their Protocol in response to a serious incident, and when the incident is over.
- The Protocol should cover the lifecycle of an incident, with measures in relation to planning, declaring an incident, managing, preventing escalation and returning to normal.

Enhance the Protocol's systems and processes

- If Ofcom considers a service provider's Protocol to not be effective or to not protect freedom of expression, it should require them to change it and support them in making it compliant.
- Ofcom should monitor the effectiveness and proportionality of measures during serious information incidents and tell service providers to take remedial steps, where needed.
- The Protocol should emphasise that it is better for service providers to declare and revoke or downgrade the severity of a serious information incident than to do nothing and let things escalate.
- The Protocol should recommend clearer remits and responsibilities as part of service providers' governance and command frameworks, as well as contingency plans to cover staff absence, training and guidance, and processes to cascade information effectively.
- Service providers should be required to test their Protocol using real-world scenarios, including their monitoring processes, response measures and recovery capabilities.

Develop the recommended response measures

- The measures recommended for responding to information incidents should include working with, and enabling the work of, independent fact checking organisations.
- Accredited fact checkers should be in scope of the data access provisions in the Data (Use and Access) Act and obtain real-time access to data, with service providers incentivised to provide meaningful access and penalised for non-compliance.
- The measures should recommend an enhanced model for Community Notes, including a system for triaging high-risk content and sending it through a high-priority funnel.
- Service providers should prioritise high-quality and public interest information during incidents, and Ofcom should oversee guidelines for those information sources.

Improve the post-crisis stage of the Protocol

- Service providers should keep written decision logs covering key actions in relation to an information incident and Ofcom should be able to review those logs where required.
- Service providers should have a framework for, and clarity over, how a decision is taken to initiate a Protocol and to determine that an incident has subsided.
- There should be a debrief session prior to the substantive post-crisis review focusing on welfare and safety, organisational or operational risks and evidence-gathering.
- Service providers should submit their post crisis-analyses to Ofcom as a matter of course, and Ofcom should scrutinise them to help drive up standards and develop best practice.
- Ofcom should make its assessment of Protocols and their implementation publicly available in summary form alongside any key recommendations.

Expand and clarify the proposed definition of 'crisis'

- The definition of 'crisis' should be clear that it can occur within the UK or any part of it, and there should be clarity about how it would be engaged at a subnational level.
- The definition should cover public health and national security as well as public safety.
- The definition or accompanying guidance should make it clear that crises can include clusters or a proliferation of claims or narratives, and that a serious information incident may build gradually and incrementally, or be sudden and acute.
- Ofcom should ensure that its definition of 'crisis' is aligned with definitions used by key public authorities to facilitate private / public coordination during serious incidents.

Assessment of the impacts, including costs

- The Protocol should be expanded to also apply to search and messaging services, and to generative AI platforms, with suitable measures for those different contexts.
- The Protocol should reflect best practice – building on existing models – and contain the most proportionate and effective measures for service providers to deal with information incidents, rather than the current framing of the *"least costly"* measures.
- Ofcom's approach to proportionality, which focuses on limiting costs for service providers, should be balanced against the nature and severity of the harms, including to individuals and society if service providers do not deal effectively with crises.

49. Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.

9. Full Fact welcomes Ofcom's consultation on the Protocol. We know that certain events can negatively affect the information environment and that misinformation can have significant consequences for individuals and society, both online and offline. This was particularly evident at the start of the Covid-19 pandemic and during the riots in summer 2024. However, whilst we support the principle of the Protocol, we are concerned that the model proposed in the consultation paper will be of limited value in the identification and management of serious information incidents in the public interest, and risks being a missed opportunity.

10. We have long advocated the need for clear, transparent protocols to tackle the spread of misinformation which cause, or result from, serious incidents. From 2020, Full Fact worked with

service providers, civil society and public authorities to create a shared model to fight misinformation crises. The resulting Framework, published on our website, is intended to help actors identify information incidents and collaborate with others to respond effectively.[3] Full Fact also has a longstanding call for the government to introduce a transparent crisis response protocol for independent management of serious information incidents during an election period, based on the model in Canada.[4] We have advocated this in annual reports, evidence to Parliamentary inquiries,[5] and as part of our ongoing efforts to ensure that the Elections Bill protects UK democracy from misinformation and disinformation.[6]

A. Improve the underlying legislative framework

11. This part of the submission considers the weaknesses of the OSA which fundamentally undermine the ability of the Protocol to tackle serious information incidents.

The Protocol is undermined by limitations of the Online Safety Act

12. The OSA should have been a pivotal moment in the way the UK tackles the harms caused by misinformation. However, it fell significantly short of the former government's original aim to make the UK *"the safest place to be online."* The proposed duty on platforms to tackle content that is 'legal but harmful' to adults was removed, and the previous government backtracked from their plan to tackle collective and societal harms, focusing instead on individuals.[7] We reiterated our position in Full Fact's 2025 report on the state of misinformation in the UK, that the OSA is not fit for purpose in tackling harmful misinformation online.[8]

13. The government recently set out its view that misinformation will be caught by the OSA where it is also a relevant offence, and that harmful misinformation for children will be caught where it intersects with priority content.[9] There is currently no credible plan to tackle the harms from online misinformation in the OSA beyond this narrow framework. This has left our democracy and society exposed to harmful misinformation online. It also means that the Protocol is being built on legislation that focuses on specific harms to individuals and which was not designed to tackle the spread of harmful misinformation or viral content.

14. We note that the government is keeping implementation of the OSA under review and we welcome their openness to going further where necessary.[10] With implementation under way, Full Fact is calling for a review to determine whether the law is capable of addressing the scale of harmful content circulating online.[11] The OSA should be amended to target systemic harms that misinformation poses to society and democracy, in line with its original ambition. Large service providers should be required to take more responsibility to identify and manage the risks of legal but harmful content, with robust safeguards for freedom of expression.

15. Whilst we recognise that such a review is beyond the scope of this consultation, the consultation paper states that the Protocol is needed because of the disorder that followed the tragic

---

[3] Full Fact (2021) Framework for Information Incidents
[4] Government of Canada(24 March 2025) Cabinet Directive on the Critical Election Incident Public Protocol
[5] Full Fact (7 September 2021) Submission to PACAC's inquiry on the Elections Bill
[6] Full Fact (1 September 2025) Blog on how the Elections Bill could protect our democracy from the harms of misinformation and disinformation
[7] UK Government (15 December 2020) Online Harms White Paper
[8] Full Fact (May 2025) 2025 Annual Report
[9] Science, Innovation and Technology Committee (9 May 2025) Letter to Baroness Jones
[10] Hansard (10 September 2025) Online Safety Act 2023: Effectiveness
[11] Full Fact (updated August 2025) What is the Online Safety Act? Here's what you need to know

murders in Southport in 2024: *"given the evidence we saw during the violent disorder following the Southport attack we consider that additional measures are necessary to address the risk of harm that may occur during a crisis faster and more effectively"*. But as set out below, the riots illustrated the limitations of the OSA in dealing with information crises and the Protocol will only be a sticking plaster without reform of the underlying law.

The Southport riots highlighted the need to improve the Act

16. Full Fact produced an overview of the role that unchecked, virally spreading, harmful online misinformation played in the riots after the attack in Southport.[12] A false claim on LinkedIn suggesting the attacker was a migrant was seen 2 million times on social media.[13] A false name of the attacker was recommended to users in the X search bar many hours after the police confirmed the name was false.[14]

17. This episode illustrated the problem with a legal framework that focuses on illegal content and individual harms, and the limitations of the false communications offence. Much of the online misinformation that fuelled the riots was not unlawful, such as the attacker's incorrect identity. The false communications offence would not apply to people who share content without knowing it is untrue, nor those who do not intend to cause physical or psychological harm, which means the offence is not suited to tackle viral online misinformation.[15]

18. On 16 October 2024, the Secretary of State for Science, Innovation and Technology wrote to Ofcom noting *"how online misinformation and incitement fuelled violence and civil unrest across the UK …. One of the most alarming aspects of this unrest was how quickly and widely content spread."*[16] Ofcom responded on 22 October 2024 setting out their conclusions: illegal content and disinformation spread widely and quickly online following the attack; there was a clear connection between online activity and violent disorder seen on UK streets; and most service providers took rapid action in response, but those responses were uneven.[17]

19. Following its inquiry into social media and misinformation, the Science, Innovation and Technology Committee ('SIT') concluded, *"The Online Safety Act was not designed to tackle misinformation—we heard that even if it had been fully implemented, it would have made little difference to the spread of misleading content that drove violence and hate in summer 2024. Therefore, the Act fails to keep UK citizens safe from a core and pervasive online harm."*[18] The review underlined the clear limitations of the OSA in dealing with information crises. In response to the SIT Committee's report, Full Fact called for a review to assess whether the OSA can combat the level of harm present on social media, for the creation of a crisis coordination framework, and for the OSA to be upgraded to tackle systemic risks.[19]

Both the Act and the Protocol should cover a wider range of content

20. We recommend that Ofcom review the content in scope of the Protocol and possibility of using content that is harmful to children to broaden the lens, and broader practical value, of the

[12] Full Fact (August 2024) What role did misinformation play in riots after the Southport stabbings?
[13] BBC (25 October 2024) How a deleted LinkedIn post was weaponised and seen by millions
[14] Institute for Strategic Dialogue (3 January 2025) Evidence to Science, Innovation and Technology Committee
[15] Online Safety Act Network (10 August 2024) Disinformation and disorder: the limits of the Online Safety Act
[16] Department for Science, Innovation and Technology (16 October 20204) Letter to Dame Melanie Dawes, Ofcom
[17] Ofcom (22 October 2024) Letter to Department for Science, Innovation and Technology
[18] Science, Innovation and Technology Committee (11 July 2025) Report on social media, misinformation and harmful algorithms
[19] Full Fact (11 July 2025) An Urgent Call for Action: Committee Report on Social Media, Misinformation and Harmful Algorithms

Protocol, such as harmful substances content. The scope of the Protocol is limited to content in the OSA and is geared specifically towards a Southport-type event. This only covers a subset of activity that could form the basis for a serious information incident, whether expected or unexpected, which might include: significant political events, environmental disasters, global or regional conflict, economic crises or health emergencies, such as the Covid-19 pandemic.

21. In our view, at a more foundational level, illegal content is too narrowly prescribed in the OSA to effectively deal with information crises. This undermines the benefits of the Protocol, which is built on a subset of that illegal content and certain content harmful to children. Pending a review of the OSA – with a view to developing a regulatory framework that deals effectively with content that is harmful to society, democracy and public health – there should be a review of whether the list of offences is sufficient.[20]

22. In its review of the police response to the riots in 2024, His Majesty's Inspectorate of Constabulary and Fire & Rescue Services ('HMICFRS') concluded that *"Given the approach taken in the Act, we question how effective the Act and regulation by Ofcom will be in the context of rapidly spreading disorder provoked by online content."*[21] HMICFRS said it appears that an offence of 'encouraging' riot or violent disorder (under Part 2 of the Serious Crime Act 2007) could be committed online – highlighting a potential gap in both the OSA and the Protocol. HMICFRS said *"it may be timely to explore whether the OSA should include specific offences relating to 'encouraging' or 'inciting' riot or violent disorder as priority offences."*[22]

B. Expand the scope and ambition of the Protocol

23. This part of the submission explores the narrow scope of the Protocol and how it could be expanded as part of a wider framework for managing information incidents.

Service providers should have a broader framework for information incidents

24. The Protocol does not consider the degrees of an information incident's severity but instead focuses on the all-or-nothing requirements of a 'crisis' as defined. The Protocol should be adapted into a broader framework for service providers to identify and manage information incidents, with crises at the severe end. Less severe incidents can still significantly impact public safety, both online and offline; and a broader framework would require service providers to address incidents before they become crises, apply suitable measures in response, and take measures after crises subside to prevent reoccurrence. This should be implemented in a way that is clear, proportionate, effective and open to public scrutiny.

25. We recommend Full Fact's Framework to Ofcom. The Framework reflects the fact that certain events are more likely to trigger information incidents and have a substantial and material impact on the people, organisations and systems that consume, process, share or act on information, towards good, neutral or bad outcomes.[23] The Framework guides users to determine the severity of an incident with indicators for the following criteria: engagement; appearance on social media, messaging services and mainstream media; languages; hashtags; search trends; influential sharing; coordinated behaviour; impact on behaviour; harm; and effect on resources. The Framework proposes five levels of severity:

[20] Full Fact (1 September 2025) Full Fact briefing on the Elections Bill
[21] HMICFRS (7 May 2025) An inspection of the police response to the public disorder in July and August 2024: Tranche 2
[22] HMICFRS (7 May 2025) An inspection of the police response to the public disorder in July and August 2024: Tranche 2
[23] Full Fact (2021) How the Framework was created

a. **Level 1**: A realistic scenario where there are low levels of misinformation. Long-term resilience building and future preparation is the focus of collaborative work, and additional responses are not needed on top of day-to-day activities.
b. **Level 2**: An incident might be emerging, and there is time to discuss what additional responses might be needed if it escalates whilst monitoring. The emerging incident may be resolved with light-touch responses before it becomes worse.
c. **Level 3**: An incident is occurring, and it is time to put in place responses discussed earlier on. Some incidents have a rapid onset, and collaborative or individual responses will need to be put in place as quickly as possible.
d. **Level 4**: A severe incident is occurring or a less severe one is becoming more serious: stringent responses are needed to contain the crisis, or existing responses need to be adapted or additional ones introduced in line with the increasing severity.
e. **Level 5**: An incident is occurring which is rare in its severity and high impact, unlikely to be resolved in the short-term, requiring maximum collaboration and response levels.

26. The Framework recognises that every incident is unique but that, in many cases, common or predictable challenges will emerge, such as threats to freedom of expression, quickly changing situations, information vacuums and uncertainty. The Framework guides users in thinking through possible aims, with a non-exhaustive list that includes: building audience resilience; communicating and debunking; disseminating accurate information; planning, coordinating and sharing information with others; restricting the spread of harmful information; and supporting the availability of reliable information from authoritative sources.

27. The Framework then proposes examples of responses that would meet these aims, such as fact checking and linking to resources, applying warnings and coordinating messaging. These would need to be adapted based on the severity of the incident and the timing: some responses will have short-term effects, others long-term ones. Different actors might come up with alternative responses based on their own experience and judgement.

28. Ofcom should ensure that the Protocol is best practice and not weaker than existing crisis response protocols. At least one service provider appears to take a broader approach than envisaged by the Protocol and looks at relative severity of incidents: in evidence to the SIT Committee's inquiry on misinformation, Meta said that it designated the initial attack in Southport under its Dangerous Organisations and Individuals policy; established a working group to follow its protocols for responding to mass violence; and designated the riots under its Crisis Policy Protocol. Meta explained that its Crisis Policy Protocol *"is a dynamic framework that allows us to identify emergent crisis situations and assess their relative severity."*[24] Service providers are able to change their approach to crises at any any point, and mandating a strong framework would help to ensure consistently high levels of diligence.

The Protocol should call for service providers to work with other stakeholders

29. The Protocol would require large service providers to establish a dedicated communication channel to law enforcement at the onset of a crisis. In our view, communication channels should be established in advance so that they can be activated in a crisis, and not just by large service providers. In addition, the Protocol does not call for engagement with the wider group of stakeholders that is needed to effectively tackle serious information incidents.

[24] Meta (9 April 2025) Evidence to the Science, Innovation and Technology Committee

30. As we set out in our evidence to the SIT Committee's inquiry on misinformation, we believe that Ofcom should coordinate a centralised framework for information incidents.[25] In this role, Ofcom should be a point of contact to support information-sharing between service providers and others during serious incidents; and provide guidance and advice on best practice through supervision of protocols and their implementation (see further below). If service providers were required to notify Ofcom that they have identified a serious incident and initiated their Protocol, Ofcom would be in a position to notify other service providers and stakeholders.

31. Irrespective of whether Ofcom takes on this role, the Protocol should require all service providers in scope to have a crisis communication plan, with clear responsibility and lines of communication to use where appropriate with: other service providers, the police, Ofcom, government departments and agencies, such as the National Security Online Information Team, civil society and grassroots organisations, and the media. Service providers should be required to consider which to engage with other actors, which might include healthcare authorities, industry bodies, humanitarian organisations or others, depending on the context.

32. In their review of the policing response to the 2024 riots, HMICFRS noted that Ofcom and the Department for Science Innovation and Technology ('DSIT') were identifying content that could affect public safety and policing; the National Police Chiefs' Council appointed a liaison officer to support information-sharing; and Ofcom worked with service providers to understand what action they were taking.[26] TikTok agreed with HMICFRS that improvements were needed in liaison and support arrangements between service providers, the police and government departments. Meta expressed concern that communication and support arrangements in major incidents could be fragmented and difficult to access: *"This caused delays, which adversely affected the initial effectiveness of communication during the period of disorder. Meta told us that the company would support the introduction of an improved and mutually understood communication network between relevant organisations."*[27]

33. HMICFRS concluded that arrangements to improve liaison and support – between the police service, government departments and service providers – are not properly established and mutually understood. They found that *"It is vital that the police service, government departments and online content providers agree and implement clear liaison and support arrangements. Otherwise, there is a serious danger that online content that represents a risk to public safety could be missed or responded to too late."*[28] The Protocol risks compounding this lack of coordination by siloing service providers from this wider ecosystem.

34. Ofcom should also require service providers to have clear processes for informing their users when a Protocol has been activated to address a serious information incident, when that incident has concluded, and what this means in practical terms for their use of the service. This should be part of the crisis communication plan. If service providers do not inform their users about a change in the service and/or they notify them after the event, there is a risk of fostering mistrust and misunderstanding, or creating the perception of a conspiracy.

The Protocol should cover the lifecycle of a crisis

[25] Full Fact (18 December 2024) Evidence to the Science, Innovation and Technology Committee
[26] HMICFRS (7 May 2025) An inspection of the police response to the public disorder in July and August 2024: Tranche 2
[27] HMICFRS (7 May 2025) An inspection of the police response to the public disorder in July and August 2024: Tranche 2
[28] HMICFRS (7 May 2025) An inspection of the police response to the public disorder in July and August 2024: Tranche 2

35. The consultation paper acknowledges that *"crises unfold in stages"* and says the Protocol will mitigate risks *"at each stage of an unfolding crisis"*. But there is insufficient emphasis on the preventative measures that service providers should take before a serious information incident, and after it has happened. Effective pre-crisis policies and procedures will help to prevent an incident happening and mitigate the risk of an incident escalating to a crisis.

36. DSIT's incident response guidance[29] and the Home Office's critical incident management framework[30] both encompass the lifecycle of an incident. In the Home Office's framework, the lifecycle of a critical incident involves planning, recognising and declaring it, managing it and preventing further escalation, and returning to normality. It recommends risk assessments when moving between stages and mitigating or addressing issues before moving to the next stage. The Protocol should similarly be structured to cover the lifecycle of an incident, with recommended measures for each phase that build on the proposals in the paper.

C. Enhance the Protocol's systems and processes

37. This part of the submission considers how to improve the systems and processes that form part of the Protocol in order to increase its effectiveness.

Ofcom should exercise a supervisory role over service providers' protocols

38. Under Article 48 of the Digital Services Act ('the DSA'), the Commission may initiate the drawing up, testing and application of voluntary crisis protocols, focused on extraordinary circumstances affecting public security or public health.[31] The Commission must aim to ensure that protocols include one or more suggested measures; and that the protocols include other specified measures, including clear procedures for determining when a protocol is to be activated, and the crisis period during which measures are to be taken. If a protocol fails to effectively address a crisis situation or safeguard the exercise of fundamental rights, the Commission can ask a provider to revise it, including by taking additional measures.

39. The Protocol gives service providers broad discretion to develop their own protocols based on a range of recommended measures. In our view, Ofcom should actively help to ensure that protocols are proportionate and effective in addressing crises and other information incidents, and strike a balance that protects freedom of expression. If service providers notify Ofcom when their protocols are initiated, and provide their post-crisis reports as a matter of course (see further below), Ofcom would be better placed to play this role. If a protocol is not effective or does not protect freedom of expression, Ofcom should tell service providers and support them in making it more compliant with freedom of expression guidance.

40. Under Article 36 of the DSA, where a crisis occurs the Commission has the power to monitor the application of measures. Where it considers measures to not be effective or proportionate, it may require providers to review or cease them. Ofcom should similarly have the power to monitor the effectiveness and proportionality of measures during serious information incidents, and to require service providers to take remedial steps. As with the Home Office's framework for managing critical incidents, the Protocol should make it clear that it is better for service providers to declare and revoke (or downgrade the severity of) a serious information incident than to do

[29] Department for Science, Innovation and Technology (updated 6 March 2024) Incident response guidance
[30] Home Office (15 July 2024) Critical incident management
[31] Article 48, Digital Services Act (November 2022) Digital Services Act

nothing and let things escalate; and should emphasise the need for service providers to act promptly when declaring an incident and implementing the Protocol.

41. Whilst Ofcom may be able to scrutinise decisions taken by certain service providers through its supervisory relationships (such as their decision to initiate or not initiate a Protocol, or the effectiveness of measures taken), this would focus on the highest reach or highest risk services. It would not be satisfactory for Ofcom to rely on these supervisory relationships to oversee the design and implementation of Protocols by all in-scope service providers.

The Protocol should recommend clear command and governance structures

42. The consultation paper recommends that the Protocol should include details of a crisis response team made up of representatives from relevant internal teams, with individuals of sufficient seniority to facilitate timely decision-making. In our view, it should recommend governance and command frameworks with clear remits and responsibilities, including for determining an incident, initiating a Protocol, and strategic and operational oversight of it, and that service providers have contingency plans to cover relevant staff absence. Staff should be trained to ensure that they are aware of relevant policies, guidance and legislation.

43. A standard command and governance structure is used for managing critical incidents and preventing escalation within government (see for example, DSIT's framework for incident response[32] and Home Office critical incident management framework).[33] This involves senior individuals with clearly defined remits: a gold (strategic) commander with ultimate responsibility for handling an incident; silver (tactical) commander/s responsible for producing a tactical plan following the strategy set by the gold commander; and bronze (operational) commander/s making operational decisions to accomplish the tactical plan.

44. Whilst the command and governance structure will depend on the size and structure of each company, and should retain some level of flexibility to adapt to crisis situations, the Protocol could go further in helping to ensure that the architecture is established before an incident happens, that the remits and areas of responsibility of senior decision-makers are understood, that there are established processes to make decisions and cascade information promptly, that there is clear accountability, and that there is collaboration and communication between service providers and other stakeholders during an information incident.

Service providers should be required to test and refine their protocols

45. The consultation paper says that protocols should be improved over time but only relies on a post-crisis analysis to achieve that. This means a Protocol would only be tested when it is used. In May 2024, the Chair of the European Risk Management Council emphasised the need for crisis management frameworks to be tested in regular dry runs, including contingency planning and governance frameworks.[34] The government's Emergency Planning Framework also emphasises the need for planning: *"Until an emergency plan has been tested, it is impossible to be sure it will work effectively in the heat of a crisis. Practising and testing all aspects of emergency plans is therefore a key part of crisis preparedness, not only to identify and address any weaknesses*

[32] Department for Science, Innovation and Technology (updated 6 March 2024) Incident response guidance
[33] Home Office (15 July 2024) Critical incident management
[34] FT (2 May 2024) Crisis management: the last line of defence

in advance, but also to help the organisation and its staff to become aware of and comfortable with their individual roles."[35]

46. The Protocol should recommend that service providers test their protocols, including their monitoring, response measures and recovery capabilities. This will enable them to identify gaps and where policies and processes can be improved before a crisis is underway.[36] This testing should be realistic so the real-world impacts are clear, with detailed records preserved. This would reflect elements of Article 48 of the DSA, which enables the Commission to involve Member States' authorities and Union bodies, offices and agencies in drawing up, testing and supervising the application of service providers voluntary crisis response protocols.[37]

47. In our joint paper with Demos, we recommended that expert groups from civil society (which should include fact checkers), academia, regulators, and government departments should map the threat landscape in order to develop targeted tools to most effectively address vulnerabilities and counter threats. As part of this, we recommended using extended hypothetical scenario mapping and exercises which deliberately explore a scenario from an adversary's perspective.[38]

D. Develop the recommended response measures

48. This part of the submission looks specifically at the measures that Ofcom recommends service providers take in response to a serious information incident.

Emphasise the importance of working with independent fact checkers

49. The measures should include a recommendation for service providers to work with, and enable the work of, independent fact checking organisations, to reduce the risk of information incidents from arising in the first place and to help manage and mitigate them when they occur. During volatile incidents like the 2024 riots, Full Fact is among the few fact checking organisations – and one of just four Meta partners in the UK – that can counter the spread of misinformation directly at the source. We published a detailed explainer outlining some of the key questions posed by the riots, which we updated in the days after, and distributed our fact checks to leading national media outlets to maximise their visibility and impact when it mattered most.[39]

50. Following Meta's announcement to end its Third-Party Fact Checking Programme in the United States in early 2025, Full Fact responded that *"locking fact checkers out of the conversation won't help society to turn the tide on rapidly rising misinformation."*[40] By partnering with service providers, fact checking organisations are able to reach and dispel massive amounts of misinformation to audiences that might otherwise be deceived. Since partnering with Meta in January 2019, to January 2025, Full Fact checked 2,596 cases which include misleading, faked, or potentially harmful posts on Facebook and other platforms.[41] We added context and provided credible information directly to thousands of posts, and anyone who saw them. We believe our fact checking played a vital role in combatting misinformation during the Southport riots. Our

---

[35] Government Communication Service (2018) Emergency planning framework
[36] Department for Science, Innovation and Technology (updated 6 March 2024) Incident response guidance
[37] Article 48, Digital Services Act (November 2022) Digital Services Act
[38] Demos / Full Fact (17 July 2025) Community Disorder: How do we prevent an information emergency?
[39] Full Fact (May 2025) 2025 Annual Report
[40] Full Fact (7 January 2025) Full Fact responds to Meta ending support for US fact checkers
[41] Full Fact (9 January 2025) How our fact checking work with Meta makes a real-world difference

teams countered many of the harmful claims that were spreading and produced checks and explainers to outline what was occurring.[42]

51. In evidence to the SIT Committee's inquiry on misinformation, Meta said their *"technology and protocols played a positive role in reducing the spread of harmful content during the crisis, distinguishing our platforms from others where such content was more prevalent."*[43] Steps to limit potentially harmful content included *"reducing the visibility of misleading content marked by third-party fact-checkers as containing the false name of the Southport perpetrator."*[44] In the lead up to the EU's 2024 Parliament Elections, Meta emphasised the effectiveness of its own labeling system, stating: *"Between July and December 2023, for example, over 68 million pieces of content viewed in the EU on Facebook and Instagram had fact checking labels. When a fact-checked label is placed on a post, 95% of people don't click through to view it."*[45]

52. Fact checkers are always important for the information environment; in a crisis situation we become more important because we can work at speed and be a trusted source. We recognise that Ofcom cannot require service providers to change their partnership policies to mandate working with fact checkers – just as it cannot change the OSA. We have set out these issues, alongside the recommendations for improving the Protocol, to underline the need for wider reforms to achieve more effective management of serious information incidents.

Accredited fact checkers should receive access to service providers' back-end data

53. In order for fact checkers to effectively target the most harmful and far-reaching claims – and to best understand how misinformation spreads – they require cooperation and access to back-end data from service providers. Access to this data in real-time would help fact checkers assess how false and harmful information can lead to information incidents. Full Fact has long called for data access.[46] This could come from platform users, algorithms or trust and safety teams. The greater the access, the more effectively we can identify and prioritise the most harmful content as it spreads, to maximise the impact of interventions and help mitigate crises. Without receiving data at scale, it is harder to mount a coordinated, timely response to falsehoods that threaten public safety, as was illustrated during the riots in summer 2024.

54. The Data (Use and Access) Act may open up data-sharing, but the criteria for qualifying as a researcher are still subject to government clarification and it remains unclear whether fact checkers will be included under this definition. Full Fact has called for fact checkers to be explicitly included, ideally verified through recognised accreditation bodies such as the International Fact Checking Network and the European Fact Checking Standards Network. Without a clear legal definition, there is a risk that platforms – particularly those based in the United States – will arbitrarily block fact checkers from accessing their platforms. The government should guarantee that fact checkers are in scope of the new regime and create incentives for companies to provide meaningful access to fact checkers. The law should also include enforceable penalties for service providers that fail to cooperate.

Recommend an enhanced model for Community Notes

---

[42] Full Fact (12 August 20204) UK riots fact checked: latest updates and key questions answered
[43] Meta (18 December 2024) Evidence to the Science, Innovation and Technology Committee
[44] Meta (9 April 2025) Evidence to the Science, Innovation and Technology Committee
[45] Meta (25 February 2024) How Meta Is Preparing for the EU's 2024 Parliament Elections
[46] Full Fact (2020) Full Fact 2020 Annual Report

55. Meta's introduction of a Community Notes model – which uses a community-based approach to provide context or correction to information online – reflects a broader shift in service providers' approach away from working with fact checkers. As the Full Fact 2025 report explained, Community Notes-style systems can be part of a wider solution, but crowdsourcing opinions and showcasing competing points of view is no substitute for independent fact checking.[47] Community Notes on X and Meta are only shown if they achieve consensus across ideologically diverse raters: Notes are approved which receive support *despite* the ideological leaning of users. This 'bridging algorithm' has theoretical strengths, but in practice it often means Notes do not get published, especially when they relate to controversial or politically charged topics. This has been demonstrated in a series of civil society reports:

    a. A review by Demos in July 2025 found that Community Notes failed to mitigate the harmful, inaccurate information that fuelled the riots in summer 2024.[48] Community Notes were largely invisible to users during the riots; where they appeared, they relied on traditional fact checking; Community Notes were too slow to prevent false and harmful information going viral; they did not prevent harmful, false rumours about the attacker amassing millions of views; and hate speech remained on X despite the use of both Community Notes and professional moderation teams.
    b. In October 2024, the Centre for Countering Digital Hate reported that *"74% of accurate community notes on US election misinformation never get shown to users."*[49]
    c. A study by Maldita during the 2024 EU election concluded that less than 15% of the tweets containing electoral disinformation had a visible Community Note and, among the 20 most viral debunked posts that received no action from the major digital platforms, 18 were on X with over 1.5 million views each.[50]

56. The consultation paper recommends that service providers build flexibility into the resourcing of their content moderation function, and increase human content moderation resources. In our view, the Protocol should recommend that service providers consider how effective their content moderation features are (including Community Notes) in tackling the spread of harmful misinformation during information incidents, before a crisis is underway. Full Fact has developed a model for Community Notes to work alongside and complement independent fact checking, which we commend to Ofcom.[51] The Protocol should draw from this and recommend that service providers adopt a crisis protocol for Community Notes systems to triage high-risk content and send it through a high priority funnel, avoiding the likelihood of ideological gridlock which X and Meta's bridging algorithm often creates.

Recommend prioritising high-quality and public interest information

57. The previous government's 2019 Online Harms White Paper, which treated online disinformation and misinformation as types of harm, proposed that *"companies will need to take proportionate and proactive measures to help users understand the nature and reliability of the information they are receiving, to minimise the spread of misleading and harmful disinformation and to increase the accessibility of trustworthy and varied news content."*[52]

---

[47] Full Fact (May 2025) 2025 Annual Report
[48] Demos (15 July 2024) Researching the riots: An evaluation of the efficacy of Community Notes during the 2024 Southport riots
[49] Centre for Countering Digital Hate (October 2024) Rated not Helpful
[50] Maldita (June 2024) Platform Response to Disinformation during the EU Election 2024
[51] Demos / Full Fact (17 July 2025) Community Disorder: How do we prevent an information emergency?
[52] UK Government (April 2019) Online Harms White Paper

58. As we set out in our submission to the Digital, Culture, Media and Sport Subcommittee's inquiry into misinformation and trusted voices, good information, from authoritative trusted sources is essential for informed public debate.[53] Where there is a lack of quality information on issues of public concern, online discussion can be dominated by speculation, low-quality or partial information, and misinformation or disinformation. The problems that can arise with information vacuums and the absence of authoritative information can be exacerbated at times of crisis. Google previously provided users with warnings about low-quality search results resulting from data voids, but the feature was removed shortly before the 2024 US election.[54] Crises can increase the complexity of accurate information, create confusion or reveal information gaps – which can increase the volume and spread of misinformation.

59. The Protocol focuses on identifying relevant illegal and/or harmful content. To address and mitigate information incidents, we recommend that it should also call for the prioritisation of high-quality and public interest information. As noted above, the Framework suggested ways to help improve the information environment during information incidents, including contextualising information and providing alternative trustworthy sources of information; and ensuring that accurate information is disseminated appropriately to public and affected groups, for example, by actively promoting alternative coverage from trustworthy sources.

60. We note that at least one service provider prioritised information quality in crises. In evidence to the SIT Committee's inquiry on misinformation, Google said *"For topics where quality information is particularly important, such as crisis situations, we place an even greater emphasis on factors related to expertise and trustworthiness. We use external search quality raters to evaluate our results and ensure they reflect what people around the world consider to be high quality, and we are transparent about how we define high quality results."*[55]

61. The Council of Europe published guidance in December 2021 on the prioritisation of public interest content.[56] The guidance sets out principles for service providers to decide, fairly and transparently, on the prominence of public interest content. This could inform guidelines, to be developed by Ofcom with input from experts, for service providers to determine high-quality and reliable sources of information to prioritise during an information incident.

E. Improve the post-crisis stage of the Protocol

There should be an emphasis on record-keeping and decision-making logs

62. The consultation paper recommends that service providers keep a written record of their post-crisis assessments. However, it does not emphasise the need for service providers to keep detailed records throughout the implementation of the Protocol, including decisions taken in the lead up to and during the crisis period. This narrow focus on record-keeping reduces scope for accountability and for service providers and Ofcom to learn lessons. In turn, this has consequences for Parliament's scrutiny of Ofcom and ability to hold it to account.

63. The Protocol should recommend that service providers keep written decision logs covering actions taken prior to, during and in light of an incident, to the extent that this does not disrupt the implementation of the Protocol. These should be prepared with a view to informing the post-

[53] Full Fact (September 2022) Evidence to the Digital, Culture, Media and Sport Subcommittee
[54] Platformer (24 February 2025) Google gives up on data voids
[55] Google (15 January 2025) Evidence to the Science, Innovation and Technology Committee
[56] Council of Europe (2 December 2021) Guidance note on the prioritisation of public interest content online

crisis stage, and be open to scrutiny by Ofcom where required to help it improve standards across the board. The Home Office's critical incident management framework requires decision logs to be taken, with accurate, complete, detailed decisions logs needed for managing an incident. It requires every decision to be logged to ensure the rationale can be recorded accurately, including options or contingencies that were considered at the time. These written logs are made available to those overseeing the post-crisis review.[57]

64. The consultation paper envisages that the Protocol would be engaged by spikes in content that could constitute criminal activity. The Protocol should therefore reflect the need for service providers to capture and store data gathered during implementation of the Protocol, with minimum standards to facilitate work with law enforcement where appropriate.

There should be metrics and a decision-making framework to determine the end of a crisis

65. The consultation paper proposes indicators for identifying a crisis and recommends that once a crisis is over, or after 90 days if sooner, service providers conduct and record a post-crisis analysis. However, it does not recommend that service providers have a decision-making framework to determine, transparently and accountably, that a crisis has concluded. Without a clear framework, service providers will not know when that 90-day period starts.

66. The Protocol should recommend that service providers have indicators and carry out a risk assessment to determine when a crisis is over or has subsided, such that they can move to a lower level of severity and take the appropriate measures in response. One of the advantages of the Framework produced by Full Fact is that it guides users to move between levels of an information incident, both up and down, using pre-established indicators and a clear range of metrics. An incident may ebb and flow in terms of its severity but the Protocol does not account for this, focusing instead on a crisis and the period after a crisis.

67. In addition, it is not clear in the Protocol who would formally determine that a crisis has started or finished, or by what means, such that the 90-day period would be triggered. A clearer command and governance structure could address this uncertainty, and should make clear to whom that decision – and other key decisions leading up, during, and after the information incident – should be communicated, both internally and, where necessary, to Ofcom. A framework that uses degrees of severity with clear indicators, and requires service providers to undertake risk assessments to move between levels, would help to avoid indefinite crises and/or the potential misuse of measures stemming from the Protocol.

There should be an initial debrief prior to the substantive post-crisis review

68. The consultation paper recommends the conclusion of a crisis or 90-day period as being reasonable for service providers to put in place more stable systems and processes once the initial demand associated with the crisis has lessened. However, this proposal does not address the fact that information incidents may be longlasting, nor that it would be desirable for service providers to consider their response and any risks straight after a crisis.

69. In our view, the Protocol should recommend an initial debrief led by a senior individual overseeing the strategic response and involving everyone who played an active part in a crisis or serious incident. This should take place as soon as possible after the incident has resolved if

[57] Home Office (15 July 2024) Critical incident management

it is acute; or soon after response measures have been implemented if the incident appears to be chronic, to the extent that this does not interfere with the service provider's response. The debrief should focus on welfare and safety, organisational or operational risks, and gathering evidence to help inform a more substantive review and to learn lessons.[58]

70. This initial debrief exercise should precede the more substantive post-crisis analysis, which is recommended in the consultation paper to take place after the incident concludes or after a 90-day period, whichever is sooner. The post-crisis analysis should review the incident (how it occurred, the impact, the responses taken, the timeline of events), what worked and areas for improvement, learning opportunities, and how to prevent a similar incident. It should lead to a written action plan for each key lesson with clear responsibilities and timelines.[59]

Post-crisis reports should be submitted to Ofcom as a matter of course

71. The consultation paper expressly does not recommend that service providers submit their post-crisis analysis to Ofcom or publish it – but Ofcom may request the analysis and its findings if considered necessary, for example, to exercise regulatory or enforcement functions. In our view, this approach is mistaken. The Protocol should require service providers to submit their post crisis-analyses to Ofcom as a matter of course. This would increase accountability for decisions made during and after the incident, and help Ofcom to drive up standards by providing guidance and advice to service providers with a clearer understanding of what worked, or did not work, in the context of different incidents and organisations.

72. We recommend that Ofcom establish a process for reviewing service providers' Protocols on an ongoing basis, and to review their effectiveness in practice after serious information incidents. Ofcom should make it clear to service providers that it may also need to scrutinise Protocols and decision-making logs, as well as post-crisis analysis reports. Post-crisis reports should include some standard requirements for reporting, such as impact on a service provider's performance, to ensure that the reports are meaningful and enable comparisons over time and between services. Regulatory scrutiny of the models, processes and their usefulness in addressing information incidents should be made publicly available in summary form alongside any key recommendations. This would inform public understanding about how well companies are addressing significant threats to the public interest.

50. Do you agree with our proposed definition of 'crisis'? Please explain your reasoning, and if possible, provide supporting evidence.

73. The Protocol defines a 'crisis' an *"extraordinary situation"* which is qualified as circumstances in which there is a *"serious threat"* to public safety in the UK. A crisis therefore appears to depend on there being a serious threat, which is not defined. The paper recommends that service providers prepare a written protocol for identifying a crisis, which should include indicators to help determine whether a crisis is occurring or is likely to occur.

74. The proposed definition of a crisis covers serious threats to public safety *"in the United Kingdom"*. The paper notes elsewhere that *"nationwide riots"*, large scale terrorist attacks and/or inter-religious or inter-ethnic violence may satisfy the definition. Whilst the paper does

[58] Home Office (15 July 2024) Critical incident management
[59] Department for Science, Innovation and Technology (updated 6 March 2024) Incident response guidance

not specify that an incident must occur at a national level, the absence of clarifying detail that it could be local or regional risks the perception of an unreasonably high threshold.

75. The definition should expressly note *"the UK or any part of it"*. This would more closely reflect Article 36 of the DSA, which encompasses serious threats in the EU or in significant parts of it. The Home Office's critical incident management framework defines critical incidents as incidents and events of any scale outside of the usual business activity that can result in serious consequences, either operational or non-operational.[60] It approaches this with three categories: local, national or cross-border. National incidents have one or more local incident points, and the impact of the incident and response involves more than one command, cause major disruption to business, prevent the organisation from meeting its objectives and fall beyond capabilities of business continuity management. In going beyond national incidents, the Protocol should be clear about how it is engaged at a regional or local level.

76. The failure of the OSA to tackle health misinformation and other serious threats to public health, and the absence of relevant content that relates to public health, has contributed to a narrow definition in the Protocol geared towards aspects of public safety. In our view, and following on from our recommendations relating to the OSA, the definition of 'crisis' should cover public health and national security, as well as public safety. This would bring it into line with section 175 of the OSA which enables the Secretary of State to give a direction to Ofcom if there are reasonable grounds for believing that circumstances threaten the health or safety of the public, or national security, to use its media literacy powers to give priority to specified objectives and/or give a *"public statement notice"* to a service provider requiring them to make public steps to tackle the threat.[61] Article 36 of the DSA defines a crisis as extraordinary circumstances leading to a serious threat to public security or public health.

77. We recognise the importance of having a clear, transparent and widely understood definition of a crisis, to ensure proportionality and the use of evidence to justify the response measures. As set out above, our view is that the Protocol should be part of a wider framework for information incidents, and that a 'crisis', as clearly defined, should be determined with reference to severity indicators. The Protocol does not make allowances for the severity of an incident but approaches a crisis as something that happens and then ceases. Full Fact's Framework defines an information incident as a cluster or proliferation of inaccurate or misleading claims or narratives – which can be sudden or have a slow onset – which relate to or affect perceptions of or behaviour towards a certain event or topic happening online or offline. We recommend that the Protocol take this broader framing and note that a crisis may involve clusters or proliferations of claims or narratives, rather than just a stand-alone event, and that a crisis may build gradually and incrementally, or be sudden and acute.

78. As we set out in our joint paper with Demos, the Defending Democracy Taskforce, Joint Election Security Preparedness Unit and/or the National Security Online Information Team are already likely to have a set definition of what constitutes a critical information incident or crisis.[62] The government's Election Cell already monitors what has been described as 'information incidents' during elections and, as a result, the government has indicated there is no need for additional crisis protocols.[63] However, there is no transparency around this framework nor what amounts

[60] Home Office (15 July 2024) Critical incident management
[61] Online Safety Act (2023) Section 175
[62] Public Technology (1 July 2024) Government extends use of digital simulation for 'information incident' crisis training
[63] Ministry of Housing, Communities and Local Government (1 January 2025) Joint Election Security Preparedness Unit

to an incident.[64] We recommend that Ofcom seek insight into these definitions, and align the definition in the Protocol with government processes, to enable better coordination between the public and private sector during serious incidents.

79. In order for Ofcom to establish whether a service provider acted correctly in initiating, or not initiating, its Protocol, Ofcom would need to determine whether a relevant information incident took place. A serious incident as determined by Ofcom for the purposes of exercising its regulatory functions may differ from a service provider's own determination. This underscores the value of having widely understood indicators for the severity of an incident, to enable a shared understanding between Ofcom, service providers and other stakeholders.

51. Do you consider these measures to be effective for services that are not large services? Please provide any evidence on the role of services that are not large services during crises.

80. The consultation paper is focused on limiting costs for service providers, as we have considered below under the section dealing with impacts. In our view, however, it should reflect best practice and be based on the principles of proportionality, effectiveness, transparency and accountability. Smaller service providers may have fewer staff and resources to allocate to the development and implementation of their Protocol, but should implement processes and measures that are proportionate to their risk profile.

81. We do not agree that only large service providers should be required to set up a dedicated communication channel allowing law enforcement to contact them, for the reasons given above. We anticipate that a communication strategy that engages a wider group of stakeholders would require relatively limited resources, and it is not clear why a smaller high-risk service provider should not have an established line of communication to the police.

82. The consultation paper notes that the dissemination of illegal and/or content harmful to children content often begins on smaller services before spreading to larger services, and notes that smaller services *"can play a structural role in fostering perpetrator networks, disseminating illegal and/or content harmful to children, and catalysing offline violence in times of crises."*[65] It is not clear from the paper whether those smaller services are high-risk or if medium-risk services also catalyse crises and should be in scope of the Protocol.

52. Is there any evidence of best practice in responding to a crisis that we have not identified? Please explain your reasoning, and if possible, provide supporting evidence.

83. As set out in paragraphs 29-31 above, Full Fact recommends our Framework for Information Incidents as a broader model for managing information incidents, including crises. This was informed by our extensive experience fact checking and through engagement with experts.[66]

84. We have identified a range of other protocols, guides and frameworks for dealing with information incidents that are instructive for the design of the Protocol:

    a. In March 2024, the European Commission published guidelines under the DSA for very large online platforms and search engines to mitigate systemic risks online specifically

[64] Demos / Full Fact (17 July 2025) Community Disorder: How do we prevent an information emergency?
[65] Minzhang Zheng et al (17 April 2024) Adaptive link dynamics drive online hate networks and their mainstream influence
[66] Full Fact (2021) How the Framework for Information Incidents was created

for elections.[67] The guidelines are based on the DSA's broader scope than the OSA in dealing with systemic risks and give an insight into how a broader regime could function in the UK.

b. This submission has drawn out measures from two key government frameworks for managing incidents: DSIT's Incident Response framework[68] and the Home Office's Critical Incident Management framework.[69] It is helpful to see how these departments identify and respond to information incidents, particularly given that service providers may need to engage with them during a serious information incident.

c. More broadly, the government's Emergency Planning Framework sets out how to plan, develop and implement an effective response during a crisis. It focuses on six stages which make up the PRIMER framework: plan, rehearse, implement, maintain, evaluate and recover.[70] As noted above, the framework emphasises the importance of emergency planning, which is not reflected in the consultation paper.

d. The Canadian Digital Media Research Network, a collective of academic researchers and other experts studying digital media, developed an Information Incident Protocol for identifying and responding to information incidents.[71] The response depends on the significance, duration, urgency, sensitivity and complexity of the incident. The Network publishes details of information incidents and analyses their impact on the Canadian information ecosystem – a level of transparency that is missing from the Protocol.[72]

e. NATO's Civil Preparedness Civil Protection Group produced the Practical Guide to Public Information During a Crisis.[73] This provides a basis for common understanding among NATO nations on public information and a framework for informing the public during the preparation, response and recovery phases of a crisis. Whilst the guide is aimed at states, it proposes a framework for keeping the public informed about an information incident, which could also inform the Protocol.

53. Do you agree with our assessment of the impacts (including costs) associated with this proposal? Please provide any relevant evidence which supports your position.

85. In their report on misinformation, the SIT Committee recommended that the Protocol should include *"all online services at risk of contributing to the spread of false or harmful information, including large online social media, search and messaging services; those with smaller user numbers but high-risk profiles; and others, such as generative AI platforms."*[74] We agree and recommend that the Protocol be expanded to also apply to search and messaging platforms, and to generative AI platforms. This would require different measures to suit those contexts. The consultation paper proposes that the measures will only apply to user-to-user services *"as current evidence shows that these are predominantly where the increase and spread of relevant illegal and/or relevant content harmful to children takes place during a crisis."* But without sight of this evidence, the extent of this predominance is not clear.

---

[67] European Commission (26 March 2024) Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections
[68] Department for Science, Innovation and Technology (updated 6 March 2024) Incident response guidance
[69] Home Office (15 July 2024) Critical incident management
[70] Government Communication Service (2018) Emergency planning framework
[71] Canadian Digital Media Research Network (September 2024) Information incident response protocol
[72] Canadian Digital Media Research Network Incidents
[73] NATO Practical Guide to Public Information during a Crisis
[74] Science, Innovation and Technology Committee (11 July 2025) Report on social media, misinformation and harmful algorithms

86. We agree that the costs to service providers to implement a Protocol are likely to depend on various factors such as existing systems and processes, number of users, technical complexity, and risk for the relevant harms; and that there is a need for flexibility to enable services to implement policies which are appropriate, accurate and proportionate.

87. As the Online Safety Act Network highlighted in an earlier response to Ofcom's illegal harms consultation: Ofcom's approach to proportionality is primarily economic and seeks to avoid imposing costs on companies, despite the fact that the OSA also specifies that levels of risk and nature and severity of harm are relevant.[75] The consultation paper focuses on the costs to service providers of the Protocol and is not balanced by the cost and resource implications of harms. If service providers do not deal effectively with crises, the harms to individuals and society could be substantial, and include undermining electoral processes, cost to businesses, straining the criminal justice system, and impacts on marginalised groups.

88. The consultation paper appears to downplay the resource allocation needed to deal with a crisis, suggesting that the proposed measures *"are the least costly, least intrusive, and most effective measures to achieve the desired impact."* A more desirable emphasis would be on the most proportionate and effective measures to deal with these situations, with suitable resources allocated relative to the serious potential risks, not the least costly option. The consultation paper seeks to minimise costs for service providers notwithstanding the fact that their services may enable serious information incidents with significant consequences.

89. The consultation paper estimates that the crisis response team would comprise around 5-10 reallocated full-time members of staff plus one senior leader, depending on the size and complexity of the service. It is not clear whether this estimate is based on evidence of existing practices, but it would be a small allocation of staff for many services to deal with what is envisaged in the paper as a rare and extraordinary situation that threatens public safety. By way of example, TikTok told the SIT Committee that it established a command centre with over 100 people working around the clock in response to the unrest in summer 2024.[76] As set out above, it is essential that the Protocol does not become a weaker baseline than service providers' existing systems but instead serves to drive up standards.

90. The consultation paper notes that harm mitigation strategies and solutions may evolve based on an industry-wide standard of continual improvement through post-crisis analysis. And that setting a regulatory standard for crisis response may incentivise third-party providers to develop protocols. However, industry-wide improvements would be more likely if service providers were required to test their protocols, to share their analyses with Ofcom, and if Ofcom played a much stronger role in helping to drive best practice. Some of the recommendations in this submission would require additional resources, but we commend these further measures to achieve more robust and effective frameworks.

17 October 2025

[75] Online Safety Act Network (February 2024) Ofcom's illegal harms consultation: emerging concerns

[76] Science, Innovation and Technology Committee (11 July 2025) Report on social media, misinformation and harmful algorithms