[GB] Ofcom introduces crisis response measures under the Online Safety Act codes

IRIS 2026-6:1/18

Alexandros K. Antoniou
University of Essex

On 9 June 2026, Ofcom, the UK's communications regulator, confirmed a new set of crisis response measures that will be incorporated into its Illegal Content Codes of Practice and Protection of Children Codes of Practice under the Online Safety Act 2023 (OSA). The measures form part of Ofcom's wider implementation of the OSA and are designed to strengthen how certain online platforms respond when exceptional events generate a rapid increase in illegal content or content harmful to children, particularly where online activity poses a threat to public safety.

Ofcom has adopted a specific definition of a crisis, described as:

"*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*" (paragraph 3.18 of the Crisis response protocol).

The regulator's case is that online services can play a role in the dissemination of unlawful material rapidly and at scale, including content encouraging hatred, threats or violence, with potential consequences extending beyond the online environment. These new measures are intended for situations where standard moderation systems may be insufficient. Ofcom pointed, in particular, to evidence from previous incidents, including public disorder after the 2024 Southport attacks, where online content was identified as a likely factor in the rapid escalation of hostility and violence.

The new provisions emerged from a consultation on additional safety measures and will complement existing duties relating to illegal content and content harmful to children. Although providers remain free to adopt alternative approaches, compliance with the codes provides a recognised route to meeting the OSA duties. At the centre of this package of measures sits a recommendation that certain user-to-user services establish an internal crisis response protocol. The protocol should enable providers to identify when a crisis is occurring or likely to occur and promptly activate appropriate mitigation measures. It should include crisis indicators, monitoring arrangements, escalation pathways, deployment of

senior personnel and operational responses aimed at managing elevated risks. Providers are also expected to maintain a structured process for reviewing their response once a crisis has ended.

The crisis protocol model is designed to remain flexible: Ofcom does not mandate fixed moderation methods but gives providers examples they may adapt to their service's size, structure and risk profile. The framework is also notable for its emphasis on preparedness rather than emergency intervention by the regulator. It does not create a mechanism through which Ofcom can formally declare a crisis. Instead, providers themselves are expected to assess developments affecting their services and determine when activation of their protocols is required. Providers should, however, take account of any public statement notice issued following a direction from the Secretary of State under section 175 of the OSA when assessing whether crisis conditions may exist.

Another significant element concerns coordination with law enforcement. Certain larger services will be expected to maintain a dedicated communication channel through which police and other authorities can share crisis-related information. Reflecting a broader emphasis on information-sharing and operational coordination, this measure is intended to facilitate faster responses where illegal content is spreading during a crisis.

The measures apply only to particular categories of user-to-user services. They are directed primarily at large services assessed as presenting medium levels of risk in relation to specified harms, together with services of any size assessed as high risk. Separate provisions cover services likely to be accessed by children. The harms in scope include terrorism-related content, hate content, harassment, threats and abuse, foreign interference, and certain forms of violent content affecting children. Ofcom declined to extend the framework to broader categories such as misinformation, public-health emergencies or environmental crises where these fall outside the statutory duties established by the OSA.

The regulator also addressed concerns raised during consultation regarding freedom of expression and privacy. Specifically, Ofcom emphasised that the measures concern organisational processes rather than mandatory content-removal rules. It acknowledged that providers may face difficult decisions when balancing speed and accuracy during a crisis and recognised the possibility of increased moderation errors. Ofcom concluded that the framework remains proportionate in light of the public safety risks it seeks to address and compatible with existing privacy and data protection obligations.

The amendments will now proceed through the parliamentary process before being incorporated into the relevant codes. Once in force, they will add a new preparedness dimension to the UK's online safety framework, requiring certain services to maintain contingency arrangements for periods of heightened risk

alongside their existing moderation systems.

Ofcom statement: "Crisis response protocol" and draft consolidated version" Illegal content - Codes of Practice for user-to-user services"

https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-crisis-response-protocol