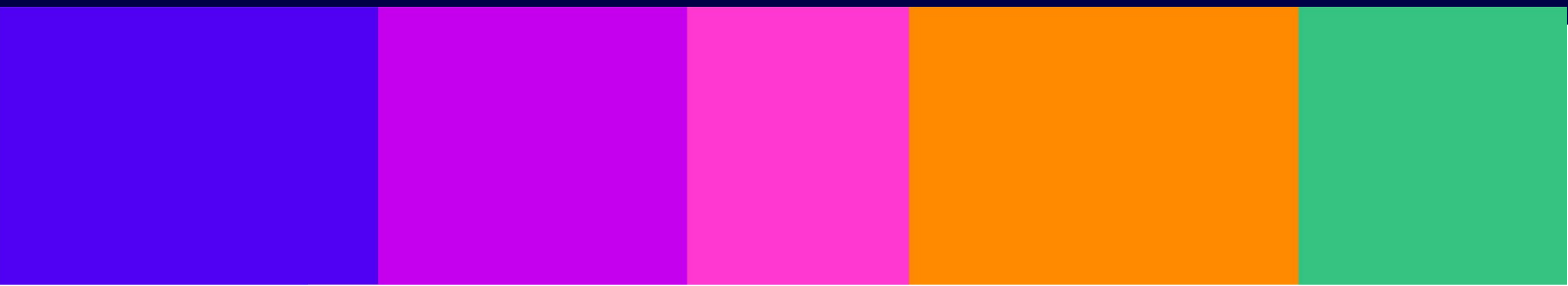




Amendments (No. 2) to the Illegal content Codes of Practice for user-to-user services

Issued: 12th October 2026

In force: 2nd November 2026

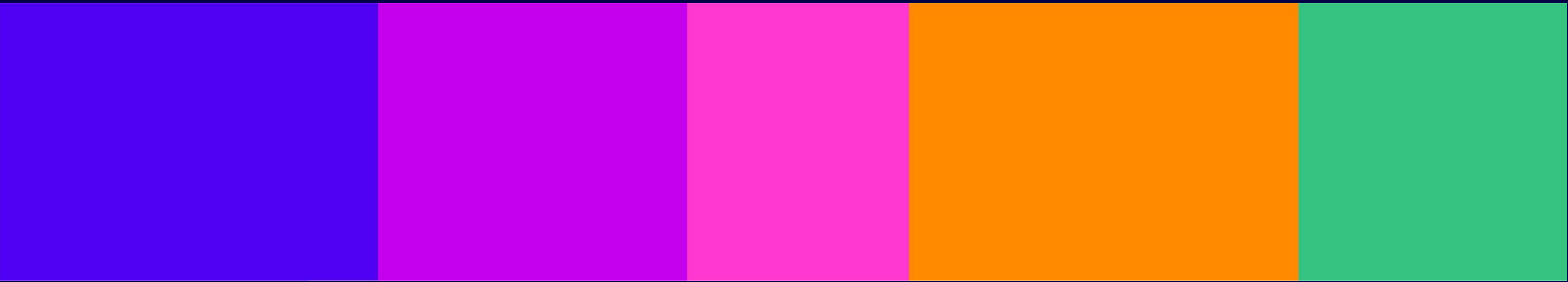


Contents

Section

1. Preamble 3

2. Amendments 4



1. Preamble

- 1.1 On 24 February 2025 Ofcom issued the Illegal content Codes of Practice for user-to-user services in accordance with section 41 of the Online Safety Act ('the Act').¹
- 1.2 Ofcom issues the amendments set out in section 2 of this notification in accordance with section 43(4) of the Act.
- 1.3 In the course of preparing the draft of amendments of those Codes, Ofcom consulted the persons mentioned in section 41(6) and (7) of that Act.
- 1.4 In accordance with section 43(2) and (3) of the Act, the draft has been laid before Parliament for the 40-day period, during which time neither House of Parliament resolved not to approve the draft.
- 1.5 The amendments come into force on 2nd November 2026 in accordance with section 43(4) of the Act.
- 1.6 Ofcom will publish the amended codes of practice on its website in accordance with section 46 of the Act.

Signed by



Jon Higham

Policy Development Director, Online Safety Group

A person authorised by Ofcom under paragraph 18 of the Schedule to the Office of Communications Act 2002

12th October 2026

¹ Ofcom, [Illegal content Codes of Practice for user-to-user services](#) (24 February 2025), as amended by ["Amendments to Illegal content Codes of Practice for user-to user services"](#) on 9 September 2026 with effect from 30 September 2026 (the "intimate image abuse amendments"). A consolidated version of the Illegal content Codes of Practice for user-to-user services incorporating amendments is published on Ofcom's website ([Online safety regulatory documents and guidance](#)).

2. Amendments

2.1 The Illegal content Codes of Practice for user-to-user services are amended as follows.

Amendments to index of recommended measures

2.2 In Section 3 (Index of recommended measures), in the appropriate places, insert the following entries—

ICU C15	Crisis response	Large services that are at medium risk of one or more specified kinds of illegal harm ; or services that are at high risk of one or more specified kinds of illegal harm .	Terrorism Other duties	Section 10(2) and 10(3)
ICU C16	Crisis response (dedicated channel for law enforcement)	Large services that are at medium or high risk of one or more specified kinds of illegal harm .	Terrorism Other duties	Section 10(2) and 10(3)

Amendments to recommended measures

2.3 In Section 4 (Recommended measures), in subsection C (Content moderation), at the end insert—

“ICU C15 Crisis response

Application

ICU C15.1 This measure applies to a **provider** in respect of each **service** it provides that meets either of the following conditions:

- a) the **service** is a **large service** at medium **risk** of one or more of the following **kinds of illegal harm**:
 - i) terrorism;
 - ii) hate;
 - iii) harassment, stalking, threats and abuse;
 - iv) the foreign interference offence; or
- b) the **service** is at high **risk** of one or more of the **kinds of illegal harm** listed in sub-paragraph (a).

Key definitions

ICU C15.2 In this Recommendation ICU C15:

“crisis” means an extraordinary situation in which there is a serious threat to public safety in the United Kingdom which is highly likely to:

- a) have resulted (in whole or in part) from a significant increase in relevant illegal content on the service; and/or
- b) have caused, or cause, a significant increase in relevant illegal content on the service;

“relevant illegal content” means **illegal content** associated with any of the following **kinds of illegal harm**:

- a) terrorism;
- b) hate;
- c) harassment, stalking, threats and abuse;
- d) the foreign interference offence.

Recommendation

- ICU C15.3 The provider should prepare and apply (but need not publish) a written internal protocol (“crisis response protocol”) to identify and respond to a crisis, for the purposes of mitigating and managing:
- a) the risks arising from a significant increase in relevant illegal content on the service during a crisis; and
 - b) where relevant, the increased risk of the service being used for the commission or facilitation of a **priority offence** during a crisis.
- ICU C15.4 The provider’s crisis response protocol should include, but need not be limited to, the following:
- a) indicators, identified by the provider, that the provider will consider in determining whether a crisis is occurring or is likely to occur;
 - b) how the provider will regularly monitor the indicators referred to in sub-paragraph (a) to determine whether a crisis is occurring or is likely to occur;
 - c) how the provider will keep the indicators referred to in sub-paragraph (a) under regular review to ensure they remain the relevant indicators to be identified in the crisis response protocol;
 - d) details of a crisis response team, including representatives of sufficient seniority from relevant internal teams, that the provider will deploy if the provider determines that a crisis is occurring or is likely to occur;
 - e) how the provider will deploy the crisis response team referred to in sub-paragraph (d) as soon as reasonably practicable if the provider determines that a crisis is occurring or is likely to occur;
 - f) systems and/or processes, identified by the provider, to mitigate and manage the risks set out in ICU 15.3(a) and (b); and
 - g) how the provider will deploy the systems and/or processes referred to in sub-paragraph (f) as soon as reasonably practicable if the provider determines that a crisis is occurring or is likely to occur.
- ICU C15.5 If Ofcom gives a public statement notice to the provider by virtue of section 175(3) of the **Act**, the provider should consider this, in addition to the indicators

referred to in ICU C15.4(a), in determining whether a crisis is occurring or is likely to occur.

- ICU C15.6 Where the provider determines that any of the indicators referred to in ICU C15.4(a) no longer remain relevant, or where new indicators are identified or existing indicators require updating, it should update its crisis response protocol accordingly.
- ICU C15.7 When the provider determines that the crisis has ended, or 90 days after the crisis began, if earlier, the provider should conduct and record (but need not publish) a post-crisis analysis recording key decisions made during the crisis and assessing whether the crisis response protocol remains appropriate for mitigating and managing the risks set out in ICU 15.3(a) and (b). The provider should then use the post-crisis analysis to make changes to the crisis response protocol, as needed, to address any identified deficiencies.

Safeguards for freedom of expression and privacy

- ICU C15.8 The following measures are safeguards to protect **United Kingdom users'** right to freedom of expression and the privacy of **United Kingdom users**:
- a) where they are applicable, Recommendations ICU C3, ICU C4, ICU C5, ICU C6, ICU C7, and ICU C8;
 - b) Recommendations ICU D1 and ICU D2; and
 - c) Recommendations ICU D8 or ICU D9 (whichever is applicable) and ICU D10.

ICU C16 Crisis response (dedicated channel for law enforcement)

Application

- ICU C16.1 This measure applies to a **provider** in respect of each **service** it provides that is a **large service** at medium or high **risk** of one or more of the following **kinds of illegal harm**:
- a) terrorism;
 - b) hate;
 - c) harassment, stalking, threats and abuse;
 - d) the foreign interference offence.

Key definitions

- ICU C16.2 In this Recommendation ICU C16:
- “crisis” means an extraordinary situation in which there is a serious threat to public safety in the United Kingdom which is highly likely to:
- a) have resulted (in whole or in part) from a significant increase in relevant illegal content on the service; and/or

- b) have caused, or cause, a significant increase in relevant illegal content on the service;

“relevant illegal content” means ***illegal content*** associated with any of the following **kinds of illegal harm**:

- a) terrorism;
- b) hate;
- c) harassment, stalking, threats and abuse;
- d) the foreign interference offence.

Recommendation

ICU C16.3 If the provider determines that a crisis is occurring or is likely to occur, it should ensure there is a dedicated channel for law enforcement to contact the provider on matters related to the crisis.”.

