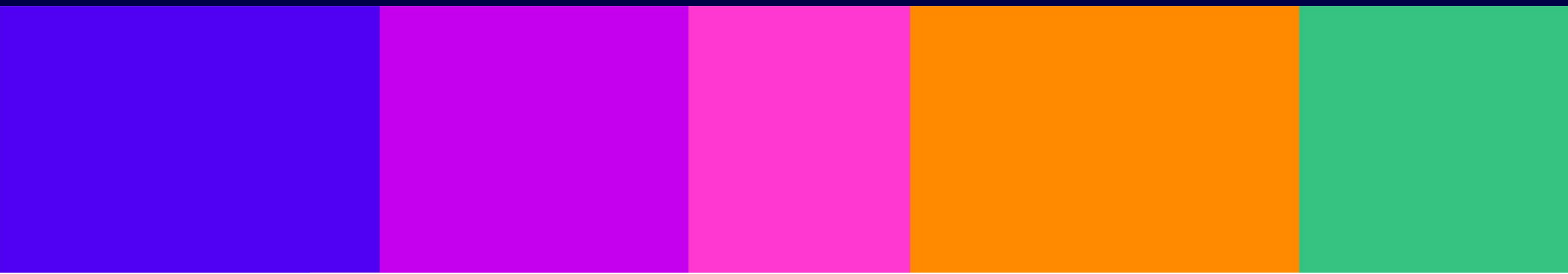




Amendments to the Protection of Children Code of Practice for user-to-user services

Issued: 12th October 2026

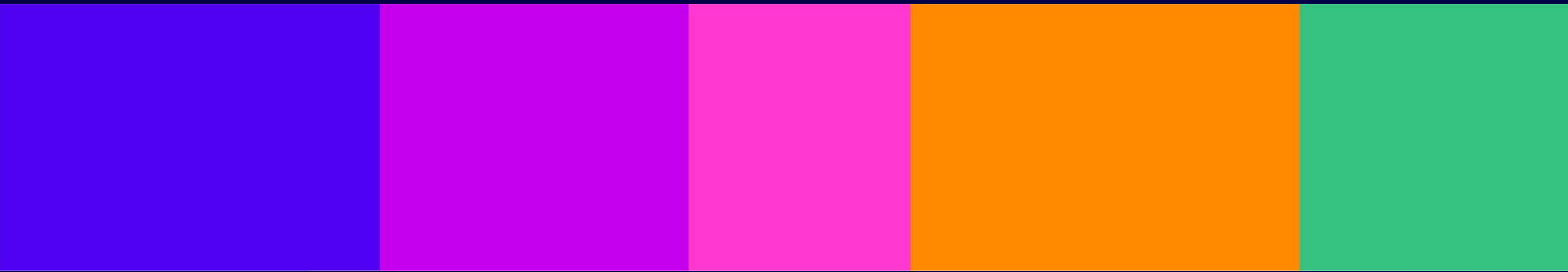
In force: 2nd November 2026



Contents

Section

1. Preamble	4
2. Amendments	5



1. Preamble

- 1.1 On 4 July 2025 Ofcom issued the Protection of Children Code 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 that Code, 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 code 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, [Protection of Children Code of Practice for user-to-user services](#) (4 July 2025). A consolidated version of the Protection of Children Code 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 Protection of Children Code of Practice for user-to-user services is 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–

PCU C11 ²	Crisis response	Services likely to be accessed by children that are either (a) a large service at medium risk of one or more specified kinds of content, or (b) a service at high risk of one or more specified kinds of content. The specified kinds of content are: abusive content, content inciting hatred, violent content (instructions for an act of serious violence against a person), and violent content (person).	Section 12(2) and 12(3)
PCU C12	Crisis response (dedicated channel for law enforcement)	Services likely to be accessed by children that are a large service at medium or high risk of one or more specified kinds of content. The specified kinds of content are: abusive content, content inciting hatred, violent content (instructions for an act of serious violence against a person), and violent content (person).	Section 12(2) and 12(3)

Amendments to recommended measures

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

“PCU C11 Crisis response

Application

² We have not used the numbering PCU C9 and PCU C10 for these amendments because Ofcom has proposed adding other Recommendations to the Code with this numbering. See Annex 9 ([DRAFT] Protection of Children Code of Practice for User-to-user services) to OFCOM’s consultation titled ‘Additional Safety Measures. Online Safety’, published on 30 June 2025 (at: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/online-safety-additional-safety-measures>).

- PCU C11.1 This measure applies to a **provider** in respect of each **service likely to be accessed by children** 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 content:
 - i) **abusive content**;
 - ii) **content inciting hatred**;
 - iii) **violent content (instructions for an act of serious violence against a person)**;
 - iv) **violent content (person)**; or
 - b) the service is at high **risk** of one or more of the kinds of content listed in sub-paragraph (a).

Key definitions

- PCU C11.2 In this Recommendation PCU C11:
- “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 harmful content on the service; and/or
 - b) have caused, or cause, a significant increase in relevant harmful content on the service;
- “relevant harmful content” means any of the following kinds of content:
- a) **abusive content**;
 - b) **content inciting hatred**;
 - c) **violent content (instructions for an act of serious violence against a person)**;
 - d) **violent content (person)**.

Recommendation

- PCU C11.3 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 the risks arising from a significant increase in relevant harmful content on the service during a crisis.
- PCU C11.4 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 arising from a significant increase in relevant harmful content on the service during a crisis; 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.

PCU C11.5 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 PCU C11.4(a), in determining whether a crisis is occurring or is likely to occur.

PCU C11.6 Where the provider determines that any of the indicators referred to in PCU C11.4(a) no longer remain relevant, or where new indicators are identified or existing indicators require updating, it should update its crisis response protocol accordingly.

PCU C11.7 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 arising from a significant increase in relevant harmful content on the service during a crisis. 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

PCU C11.8 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 PCU C3, PCU C4, PCU C5, PCU C6, PCU C7 and PCU C8;
- b) Recommendations PCU D1 and PCU D2; and
- c) Recommendations PCU D8 or PCU D9 (whichever is applicable) and PCU D10.

PCU C12 Crisis response (dedicated channel for law enforcement)

Application

PCU C12.1 This measure applies to a **provider** in respect of each **service likely to be accessed by children** it provides that is a **large service** at medium or high **risk** of one or more of the following kinds of content:

- a) **abusive content**;

- b) **content inciting hatred;**
- c) **violent content (instructions for an act of serious violence against a person);**
- d) **violent content (person).**

Key definitions

PCU C12.2 In this Recommendation PCU C12:

“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 harmful content on the service; and/or
- b) have caused, or cause, a significant increase in relevant harmful content on the service;

“relevant harmful content” means any of the following kinds of content:

- a) **abusive content;**
- b) **content inciting hatred;**
- c) **violent content (instructions for an act of serious violence against a person);**
- d) **violent content (person).**

Recommendation

PCU C12.3 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.”.

