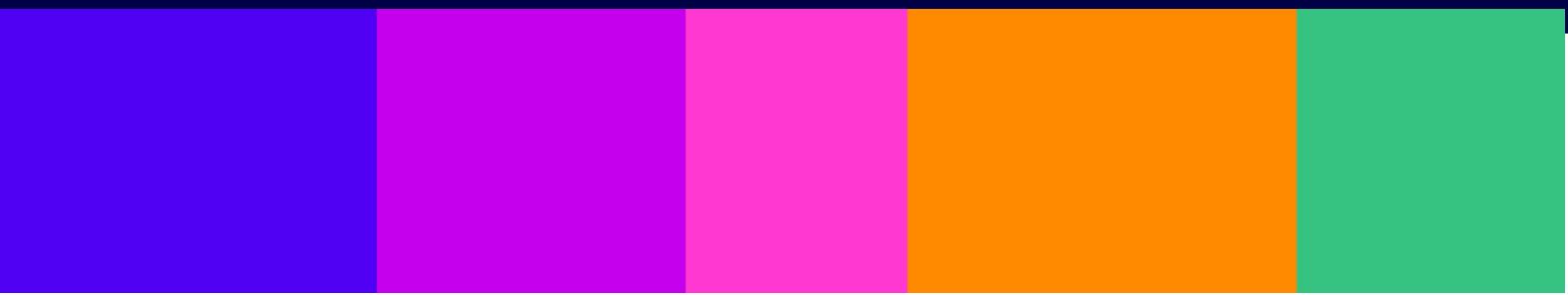


Amendments to Illegal content Codes of Practice for user-to- user services

Issued: 9 September 2026

In force: 30 September 2026

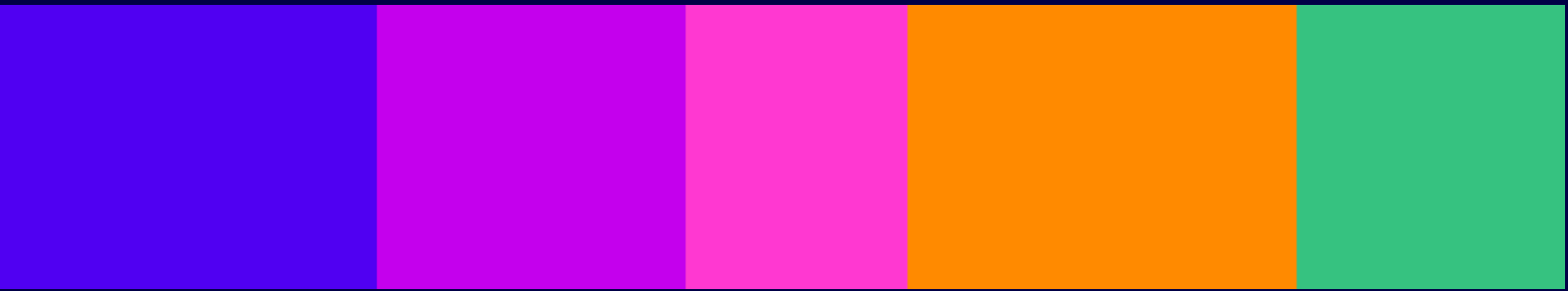


Contents

Section

1. Preamble3

2. Amendments4



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 to 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 30 September 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



Almudena Lara

Policy Development Director, Online Safety Group

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

9 September 2026

¹ Ofcom, [Illegal content Codes of Practice for user-to-user services](#) (24 February 2025).

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 C11	[Intentionally blank]	[Intentionally blank]	[Intentionally blank]	[Intentionally blank]
ICU C12	[Intentionally blank]	[Intentionally blank]	[Intentionally blank]	[Intentionally blank]
ICU C13	[Intentionally blank]	[Intentionally blank]	[Intentionally blank]	[Intentionally blank]
ICU C14	Using hash matching to detect intimate image abuse content	Services that enable <i>regulated user-generated content</i> in the form of photographs, videos or visual images (whether or not combined with written material) to be generated, uploaded or shared, and: a) are at high risk of <u>intimate image abuse</u>, and: i) the principal purpose of the service is the hosting or dissemination of regulated pornographic content; or ii) have more than 700,000 monthly active UK users; or iii) are file-storage and file-sharing services; or b) are large services at medium or high risk of <u>intimate image abuse</u>.	Other duties	Section 10(2) and (3)

Amendments to recommended measures

- 2.3 In Section 4 (Recommended measures), after Recommendation ICU C10 (Detecting and removing content matching listed CSAM URLs), insert–

“ICU C11 [Intentionally blank]

ICU C12 [Intentionally blank]

ICU C13 [Intentionally blank]

ICU C14 Using hash matching to detect intimate image abuse content

Application

- ICU C14.1 This measure applies to a **provider** in respect of each **service** it provides that enables **regulated user-generated content** in the form of photographs, videos or visual images (whether or not combined with written material) to be generated, uploaded or shared, and:
- a) is at high **risk** of intimate image abuse, and:
 - i) the principal purpose of the **service** is the hosting or dissemination of **regulated pornographic content**;
 - ii) has more than 700,000 monthly **active United Kingdom users** (see paragraphs 5.7 to 5.10); or
 - iii) is a **file-storage and file-sharing service**; or
 - b) is a **large service** and is at medium or high **risk** of intimate image abuse.

Key definitions

- ICU C14.2 In this Recommendation ICU C14:
- “relevant content” means:
- a) any **regulated user-generated content** in the form of photographs, videos or visual images (whether or not combined with written material) that:
 - i) may be **encountered** by **United Kingdom users** of the service by means of the service, and
 - ii) is communicated publicly² by means of the service; or

² Ofcom has published **guidance on content communicated ‘publicly’ and ‘privately’ under the Online Safety Act** for this purpose.

- b) any material which, if it were present on the service, would be content within sub-paragraph (a);

“unverified hash” means a hash which is not a verified hash;

“verified hash” means a hash which was determined to be of **intimate image abuse content** at the time the hash was uploaded to a database.

Recommendation

ICU C14.3 The provider should ensure that, where technically feasible, **hash matching technology** is used effectively (see ICU C14.8) to analyse relevant content to assess whether it is **intimate image abuse content**. For this purpose, the provider should use:

- a) **perceptual hash matching technology**; or
- b) where the provider’s appropriate set of hashes (as defined in ICU C14.9) does not enable perceptual hash matching for video **content**, **cryptographic hash matching**.

ICU C14.4 In circumstances where:

- a) relevant content matches with an unverified hash; and
- b) either of the following apply:
 - i) if **perceptual hash matching technology** is used, it is the first time there has been a positive match with that hash at that configuration of the technology (see ICU C14.8(b)); or
 - ii) if **cryptographic hash matching** is used, it is the first time there has been a positive match with that hash;

the provider should treat this as reason to suspect that the relevant content may be **illegal content** and review the relevant content in accordance with Recommendation ICU C1.

ICU C14.5 Where relevant content matches with a hash in circumstances other than those set out in ICU C14.4, the provider:

- a) may, depending on the level of assurance the provider has in the detection outcomes achieved by the **hash matching technology**, treat the relevant content as **illegal content** and swiftly take it down in accordance with ICU C2.3; or
- b) should otherwise treat the match as reason to suspect that the relevant content may be **illegal content** and review the relevant content in accordance with Recommendation ICU C1.

ICU C14.6 The provider should ensure human moderators review and assess an appropriate proportion of **detected content**, having regard to:

- a) the level of assurance the provider has in the detection outcomes achieved by the **hash matching technology** and any associated **systems and processes** (as indicated by the ongoing monitoring, evaluation and quality assurance (including human quality assurance) of the performance of the technology); and
- b) to the extent that **detected content** is subject to review for the purpose of Recommendation ICU C1:
 - i) the potential severity of the harm to those depicted in or **encountering intimate image abuse content**; and
 - ii) the overall impact of an incorrect decision that the relevant content is **illegal content** on a **United Kingdom user** who generated, uploaded or shared the content.

ICU C14.7 For the purposes of ICU C14.3, the provider should ensure that:

- a) all relevant content present on the service at the time the **hash matching technology** is implemented is analysed within a reasonable time; and
- b) relevant content that is generated on, uploaded to or shared on the service (or that a user seeks to so generate, upload or share) after the **hash matching technology** is implemented is analysed before or as soon as practicable after it can be **encountered by United Kingdom users** of the service.

ICU C14.8 For the use of **hash matching technology** to be effective, it should:

- a) use a suitable hash function to compare the relevant content to an appropriate set of hashes (see ICU C14.9 to ICU C14.12); and
- b) where **perceptual hash matching technology** is used, be configured so that its performance strikes an appropriate balance between **precision** and **recall** (see ICU C14.13 to ICU C14.15).

The set of hashes

ICU C14.9 For the set of hashes to be appropriate, it should:

- a) contain hashes of a significant number of original items of **content**;
- b) be proactively updated with reasonable regularity; and
- c) be secured from unauthorised access, interference and (to the extent the database is comprised of verified hashes) exploitation (whether by persons who work for that person or are providing a service to that person, or any other person).

ICU C14.10 Where the provider becomes aware of **intimate image abuse content** a hash of which is not included on any database used by the provider, the provider should

take reasonable steps to secure that a hash of that **content** is added to each such database.

- ICU C14.11 The provider should take reasonable steps to secure the removal of a hash from any hash database used by the provider where it has determined that the hash is not of **intimate image abuse content** (see ICU C14.12).
- ICU C14.12 For the purposes of ICU C14.11, the provider determines that the hash is not of **intimate image abuse content** in any of the following circumstances:
- a) the provider views the **content** used to generate the hash and determines it is not **intimate image abuse content**;
 - b) the provider otherwise reasonably believes that the hash is of **content** that is not **intimate image abuse content**;
 - c) the provider views **detected content** matched with the hash using **cryptographic hash matching technology** and determines that that **content** is not **intimate image abuse content**; or
 - d) the provider views **detected content** matched with the hash using **perceptual hash matching technology** and determines that that **content** is not **intimate image abuse content**, provided that the provider reasonably believes that there is an exact match between the hash of the **detected content** and the hash included on the database.

Technical configuration

- ICU C14.13 In configuring the **hash matching technology** so that its performance strikes an appropriate balance between **precision** and **recall**, the provider should ensure that the following matters are taken into account:
- a) the service's **risk** of harm relating to intimate image abuse, reflecting the **risk assessment** of the service and any information reasonably available to the provider about the prevalence of relevant content that is **intimate image abuse content** on the service;
 - b) the proportion of **detected content** that is a **false positive**; and
 - c) the effectiveness of the **systems and/or processes** used to identify **false positives**.
- ICU C14.14 The provider should ensure that the performance of the **hash matching technology**, and whether the balance between **precision** and **recall** continues to be appropriate, is reviewed at least every six months.
- ICU C14.15 The provider should ensure that a written record is made of how this balance has been struck in configuring the **hash matching technology**, including what information has been considered, and information about reviews and steps taken in response.

Safeguards for freedom of expression and privacy

- ICU C14.16 Paragraphs ICU C14.4 to ICU C14.6 and ICU C14.8 to ICU C14.15 of this Recommendation ICU 14 are safeguards to protect **United Kingdom users'** right to freedom of expression and the privacy of **United Kingdom users**.
- ICU C14.17 The following measures are also safeguards to protect **United Kingdom users'** right to freedom of expression and the privacy of **United Kingdom users**:
- a) Recommendations ICU C1 and ICU C2, and where they are applicable, Recommendations ICU C3, ICU C4, ICU C6, ICU C7 and ICU C8 (in relation to content moderation);
 - b) Recommendations ICU D1 and ICU D2, so far as they relate to **appeals** or complaints by **United Kingdom users** and **affected persons** if they consider that the provider is not complying with its duties in relation to freedom of expression or privacy;
 - c) Recommendations ICU D8 or ICU D9 (whichever is applicable), ICU D10 (in relation to **appeals**) and ICU D12; and
 - d) Recommendation ICU G1 (terms of service: substance (all services)).”.

Amendments to definitions and interpretation

- 2.4 In Section 5 (Definitions and interpretation), in Table A, in the appropriate places, insert the following entries—

Cryptographic hash matching technology	Technology that detects exact matches to digital content by comparing cryptographic hash values of the content against a reference database of cryptographic hash values. A match is identified only where the hash values are identical.
Hash matching technology	Either perceptual hash matching technology or cryptographic hash matching technology .
Intimate image abuse content	Content which amounts to an offence: a) under section 66B of the Sexual Offences Act 2003 (sharing or threatening to share intimate image or film); or b) under section 2 of the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 (asp 22) (disclosing, or threatening to disclose, an intimate photograph or film).

Regulated pornographic content	<i>Pornographic content</i> other than content of a type described in section 61(6) of the Act .
---------------------------------------	--

2.5 In Section 5 (Definitions and interpretation), in Table B, in the appropriate place, insert the following entry—

Pornographic content	<u>Section 236(1)</u> See the entry for “content” regarding the definition of that term.
-----------------------------	--

