Ofcom

Draft of amendments to lie before both Houses of Parliament for the 40-day period in accordance with section 43 of the Online Safety Act 2023, during which time either House may resolve that the draft be not approved.

Draft amendments to Illegal content Codes of Practice for search services

Draft of amendments prepared under section 41 of the Online Safety Act 2023 and submitted to the Secretary of State in accordance with section 43(1) on 15 May 2026.

Draft of amendments to lie before both Houses of Parliament for the 40-day period in accordance with section 43 of the Online Safety Act 2023, during which time either House may resolve that the draft be not approved.

Office of Communications

Draft amendments to Illegal content Codes of Practice for search services

Presented to Parliament pursuant to section 43(2)
of the Online Safety Act 2023

June 2026

© Ofcom copyright 2026

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at iiastatement2026@ofcom.org.uk.

ISBN 978-1-5286-6520-9

E03610761 06/26

Printed on paper containing 40% recycled fibre content minimum
Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

Contents

Section

1. Preamble 4

2. Amendments 5

1. Preamble

1.1 On 24 February 2025 Ofcom issued the Illegal content Codes of Practice for search 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.

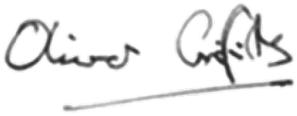
1.3 In the course of preparing the draft of amendments to those Codes, Ofcom consulted the persons mentioned in section 41(6) and (7) of that Act.

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 [*at the end of the period of 21 days beginning with the day on which they are issued*] 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



Oliver Griffiths

Group Director, Online Safety

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

15 May 2026

[1] Ofcom, Illegal content Codes of Practice for search services (24 February 2025).

2. Amendments

2.1 The Illegal content Codes of Practice for search services are amended as follows.

Amendments to index of recommended measures

2.2 In Section 3 (Index of recommended measures), in the appropriate place, insert the following entry–

ICS C8	Using hash matching to detect intimate image abuse content	**Large general search services.**	Other duties	Section 27(2) and (3)

Amendments to recommended measures

2.3 In Section 4 (Recommended measures), after Recommendation ICS C7 (Removing listed CSAM URLs from search results), insert–

"ICS C8 Using hash matching to detect intimate image abuse content

Application

ICS C8.1 This measure applies to a ***provider*** in respect of each **large general search service** it provides.

Key definitions

ICS C8.2 In this Recommendation ICS C8:

"relevant content" means any ***search content*** in the form of photographs, videos or visual images (whether or not combined with written material) that ***United Kingdom users*** can ***encounter*** in or ***via search results***;

"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

ICS C8.3 The provider should ensure that **hash matching technology** is used effectively (see ICS C8.8) 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 ICS C8.9) does not enable perceptual hash matching for video ***content***, **cryptographic hash matching**.

ICS C8.4 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 ICS C8.8(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 ICS C1.

ICS C8.5 Where relevant content matches with a hash in circumstances other than those set out in ICS C8.4, 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 take **appropriate moderation action** in relation to the relevant content in accordance with Recommendation ICS C1; 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 ICS C1.

ICS C8.6 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 ICS 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 an ***interested person*** to whom the content relates.

ICS C8.7 For the purposes of ICS C8.3, 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 may be ***encountered*** in or ***via search results*** by ***United Kingdom users*** after the **hash matching technology** is implemented is analysed before or as soon as practicable after it can be so ***encountered***.

ICS C8.8 For the use of **hash matching technology** to be effective, it should:

a) use a suitable hash function to compare relevant content to an appropriate set of hashes (see ICS C8.9 to ICS C8.12); and

b) where **perceptual hash matching technology** is used, be configured so that its performance strikes an appropriate balance between **precision** and **recall** (see ICS C8.13 to ICS C8.15).

The set of hashes

ICS C8.9 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).

ICS C8.10 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.

ICS C8.11 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 ICS C8.12).

ICS C8.12 For the purposes of ICS C8.11, 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

ICS C8.13 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.**

ICS C8.14 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.

ICS C8.15 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

ICS C8.16 Paragraphs ICS C8.4 to ICS C8.6 and ICS C8.8 to ICS C8.15 of this Recommendation ICS C8 are safeguards to protect ***United Kingdom users'*** and ***interested persons'*** right to freedom of expression and the privacy of ***United Kingdom users*** and ***interested persons***.

ICS C8.17 The following measures are also safeguards to protect ***United Kingdom users'*** and ***interested persons'*** right to freedom of expression and the privacy of ***United Kingdom users*** and ***interested persons***:

a) Recommendation ICS C1, and where they are applicable, Recommendations ICS C2, ICS C3, ICS C5 and ICS C6 (in relation to search moderation);

b) Recommendations ICS D1 and ICS D2, so far as they relate to **appeals** or complaints by ***United Kingdom users*** and ***interested persons*** if they consider that the provider is not complying with its duties in relation to freedom of expression or privacy;

c) Recommendations ICS D7 or ICS D8 (whichever is applicable), ICS D9 (in relation to **appeals**) and ICS D11; and

d) Recommendation ICS G1 (publicly available statements: 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.

Detected content	***Search content*** detected by the use of a **relevant technology** as being (or as likely to be) **target content** (and related expressions are to be read accordingly).

False positive	**Detected content** that is not **target content.**

Hash matching technology	Either **perceptual hash matching technology** or **cryptographic hash matching technology**.

Intimate image abuse content	***Search 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).

Perceptual hash matching technology	Image matching technology which compares the similarity between hashes created from images by means of an algorithm known as a perceptual hash function, to assess whether those images are perceptually similar to each other. This does not include technology which compares similarity through the use of machine learning.

Precision	A measure of statistical accuracy, calculated as the proportion of **detected content** that a **relevant technology** has correctly identified as **target content**.

Recall	A measure of statistical accuracy, calculated as the proportion of **target content** analysed by a **relevant technology** that the technology has **detected**.

Relevant technology	The kind of technology specified in the measure in question.

Target content	***Content*** of the kind the use of a **relevant technology** is designed to identify.

Classification: HIGHLY SENSITIVE

E03610761

978-1-5286-6520-9