Paper to lie before both Houses of Parliament for a period of 40 days, during which time either House may resolve that the draft code of practice be not approved.

Ofcom

Draft Illegal Content Code of Practice for user-to-user services: Proactive Technologies (unknown content)

Draft prepared under section 41 of the Online Safety Act 2023 and submitted to the Secretary of State in accordance with section 43(1) of that Act on 16 November 2026.

Paper to lie before both Houses of Parliament for a period of 40 days, during which time either House may resolve that the draft code of practice be not approved.

Office of Communications

Draft Illegal Content Code of Practice for user-to-user services: Proactive Technologies (unknown content)

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

November 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 asmconsultation@ofcom.org.uk

ISBN 978-1-5286-6893-4

E03719696 11/26

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

1. Introduction and relationship to other Codes 4

The Illegal Content Code of Practice for user-to-user services: Proactive Technologies (unknown content) 4

The recommended measures 4

Data protection 5

External documents 5

2. Application and scope 6

3. Index of recommended measures 7

4. Recommended measures 8

5. Definitions and interpretation 13

Risks of illegal harm 18

User numbers 19

1. Introduction and relationship to other Codes

The Illegal Content Code of Practice for user-to-user services: Proactive Technologies (unknown content)

1.1 Under the Online Safety Act 2023 (the 'Act'), Ofcom is required to prepare and issue Codes of Practice ('Codes') for providers of Part 3 services, describing measures recommended for the purpose of compliance with specified duties imposed on those providers by the Act.

1.2 The Act requires Ofcom to prepare and issue separate Codes for terrorism (arising from the offences set out in Schedule 5 to the Act) and child sexual exploitation and abuse ('CSEA') (arising from the offences set out in Schedule 6 to the Act) and one or more Codes for the purpose of compliance with the relevant duties relating to illegal content and harms (except to the extent measures are included in the Codes for terrorism and CSEA). Many of our recommended measures apply to more than one kind of illegal harm. To minimise duplication and simplify the regime for service providers, we produced one document, entitled "The Illegal content Codes of Practice for user-to-user services", containing the main Codes for terrorism, CSEA and other duties.

1.3 This document contains further Code measures relating to a specialist topic: the use of proactive technology to detect previously unknown image-based child sexual abuse material. The recommendations are intended to complement, rather than replace, the recommendations contained in the main Illegal content Codes of Practice for user-to-user services (including the measure on the use of hash-matching to detect child sexual abuse material). Providers should therefore consider both any specialist Codes and the Illegal content Codes of Practice for user-to-user services when determining the measures appropriate for complying with their duties under the Act.

1.4 Ofcom may from time to time amend Codes of Practice to reflect technological developments, emerging evidence, changes in risk, or other relevant developments or produce further Codes on specialist topics, which will be published on Ofcom's website (at https://www.ofcom.org.uk) [1]. Providers should ensure they check this site.

The recommended measures

1.5 Section 3 of this document sets out the recommended measures and is divided into subsections by thematic area. The meaning of terms in bold, terms in bold and italics, and terms which are underlined is explained in Section 4.

1.6 The Act provides that service providers which implement the measures recommended to them in Codes of Practice will be treated as complying with the relevant duty or duties to which those measures relate.

[1] https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/online-safety-regulatory-documents.

1.7 Service providers may seek to comply with a relevant duty in another way by adopting what the Act refers to as alternative measures. In doing so, service providers would also need to comply with the duty to have particular regard to the importance of protecting United Kingdom users' right to freedom of expression and the privacy of United Kingdom users.

1.8 Where they take alternative measures, service providers must also maintain a record of what they have done and how they consider that it meets the relevant duties, including how they have complied with the duty to have particular regard to the importance of protecting freedom of expression and privacy.

Data protection

1.9 Implementing the recommended measures set out in this Code will inevitably involve the processing of personal data. The Information Commission ('the ICO') is the statutory regulator for data protection law and has made clear that it expects service providers to comply fully with data protection law when taking measures for the purpose of complying with their online safety duties under the Act.

1.10 The ICO has set out that it expects service providers to take a 'data protection by design and by default' approach when implementing online safety systems and processes. It advises service providers to familiarise themselves with the data protection legislation, the ICO's Children's code and relevant ICO guidance, including the updated opinion published by the ICO in January 2024 setting out the Commission's expectations for age assurance under the Children's code, to understand how to comply with the data protection regime.

External documents

1.11 A hard copy of any external document referred to in the recommended measures can be obtained by writing to Ofcom at Riverside House, 2a Southwark Bridge Road, London, SE1 9HA (tel. 020 7981 3000).

2. Application and scope

2.1 This Code applies to a ***provider*** in respect of the **regulated user-to-user service** that it provides.

2.2 If a person is the ***provider*** of more than one **regulated user-to-user service**, the recommended measures in this Code have effect in relation to each such service (so far as applicable).

2.3 This Codes applies regardless of whether or not the ***provider*** of the service is inside the United Kingdom.

2.4 The services in respect of which each recommended measure in this Code applies are specified in the "application" section of each measure.

2.5 Section 5 of this document includes provision about a service's risk and size. The subsection headed 'Risks of illegal harm' (which begins at paragraph 5.4) sets out when a service is at medium or high risk of a kind of illegal harm.

2.6 The subsection headed 'User numbers' (which begins at paragraph 5.6) explains when a service is to be treated as having more than a particular number of monthly **active United Kingdom users** for those measures which apply in relation to **services** of a certain size, and how to calculate the number of monthly **active United Kingdom users**. The definition of '**large service**' is included in the definitions section in Section 5 of this document.

3. Index of recommended measures

Recommended measure		Application	Code(s)	Relevant duties
ICU PT 1	Deployment of proactive technology to detect image-based CSAM content	This measure applies to a ***provider*** in respect of each **service** it provides that is one or more of the following: a) a **large *user-to-user service*** that is at medium **risk** of image-based CSAM; b) a ***user-to-user service*** that has more than 700,000 monthly **active United Kingdom users** (see paragraphs 5.6-5.9) and is at high **risk** of image-based CSAM; c) a **file-storage and file-sharing service** that is at high **risk** of image-based CSAM.	CSEA	Sections 10(2) and 10(3)

4. Recommended measures

ICU PT 1 Deployment of proactive technology to detect image-based CSAM content

Application

ICU PT 1.1 This measure applies to a ***provider*** in respect of each **service** it provides that is one or more of the following:

a) a **large *user-to-user service*** that is at medium **risk** of image-based CSAM;
b) a ***user-to-user service*** that has more than 700,000 monthly **active United Kingdom users** (see paragraphs 5.6-5.9) and is at high **risk** of image-based CSAM;
c) a **file-storage and file-sharing service** that is at high **risk** of image-based CSAM.

Key definitions

ICU PT 1.2 In this Recommendation ICU PT 1:

"specified technologies" means ***proactive technologies*** which are:

a) **text matching technologies**, or
b) **application-specific machine learning technologies**.

Recommendation

ICU PT 1.3 The provider should ensure that, where technically feasible, it uses one or a combination of the **specified technologies** effectively to analyse **relevant inputs** for the purpose of **detecting**, or supporting **detection** of, **unknown image-based CSAM content**.

ICU PT 1.4 In selecting, and throughout the lifecycle of, the **relevant technology** concerned, the provider should ensure that it meets the following criteria (collectively, the "proactive technology criteria"):

a) ICU PT 1.5 (high-quality data),
b) ICU PT 1.6 (addressing biases),
c) ICU PT 1.7 (evaluating performance),
d) ICU PT 1.9 (safeguards against misuse and exploitation),
e) ICU PT 1.10 (contextual testing and evaluation),
f) ICU PT 1.11 (maintenance and ongoing monitoring),

g) ICU PT 1.12 (human review), and
h) ICU PT 1.14 (incorporating feedback).

ICU PT 1.5 The high-quality data criterion is fulfilled if the **relevant technology** has been developed and tested using high-quality datasets appropriate to and reflecting a broad range of inputs relevant to the harm it is intended to **detect** (as identified in the provider's **risk assessment**).

ICU PT 1.6 The addressing biases criterion is fulfilled if:

a) potential biases have been identified and addressed, and
b) risks are appropriately managed and addressed throughout the **relevant technology's** lifecycle.

ICU PT 1.7 The evaluating performance criterion is fulfilled if:

a) the **relevant technology** has been evaluated using appropriate performance metrics, and
b) configured so that its performance strikes an appropriate balance between **precision** and **recall**.

ICU PT 1.8 An appropriate balance of **precision** and **recall** is a balance set with a view to minimising the incidence and impact of moderation errors including both failures to identify **image-based CSAM content** and incorrect action against content. When configuring the technology so that it 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 **image-based CSAM**, reflecting the **risk assessment** of the service and any information reasonably available to the provider about the prevalence of **target content** on the service,
b) the proportion of **detected content** that is a **false positive**,
c) the effectiveness of the ***systems and/or processes*** used to identify **false positives**, and
d) the importance of minimising the reporting of **false positives** to the National Crime Agency (NCA) or a foreign agency.

ICU PT 1.9 The safeguards against misuse and exploitation criterion is fulfilled if safeguards are in place to identify and appropriately manage security threats and risks of exploitation and misuse, including through the use of access restrictions and system integrity protections.

ICU PT 1.10 The contextual testing and evaluation criterion is fulfilled if:

a) the **relevant technology's** performance has been evaluated in real-world use cases relevant to the provider's content (having regard to the **risk** of harm to individuals identified in the provider's **risk assessment**), and
b) the results indicate that it correctly **detects** the harm it is intended to **detect**.

This evaluation includes testing for scalability, handling of different media types (where relevant), and assessing whether the **relevant technology's** performance could be improved by layering with complementary approaches or (in the case of existing deployments) by updating to a more current version.

ICU PT 1.11 The maintenance and ongoing monitoring criterion is fulfilled if mechanisms are in place to monitor, maintain and quality assure the **relevant technology's** effectiveness over time, including processes for regular review, quality assurance and iterative adjustments to respond to emerging circumvention techniques, biases, or new content types.

ICU PT 1.12 The human review criterion is fulfilled if:

a) policies and processes are in place for human review for both moderation and quality assurance purposes, and
b) the provider abides by its policies and follows its processes.

ICU PT 1.13 For the purposes of complying with ICU PT 1.12, providers must:

a) for moderation purposes, ensure the human review of an appropriate proportion of the outputs of the **relevant technology** during deployment,
b) for quality assurance purposes, throughout the lifecycle of the **relevant technology**, ensure the human review of an appropriate proportion of the outputs of the proactive technology and of **undetected content**,
c) ensure outputs are explainable to the extent necessary to support meaningful human judgement and accountability, and
d) when determining what is an appropriate proportion of outputs of the **relevant technology** and **undetected content** (where applicable) to be reviewed by humans, ensure that the following matters are taken into account:

    i) the level of assurance the provider has in the detection outcomes produced by the technology and any **associated systems and processes**,

    ii) the potential severity of the harm to those depicted in or encountering **image-based CSAM content**, and

    iii) for moderation purposes, the overall impact of an incorrect decision that the content is **image-based CSAM content**, on the user who generated, uploaded or shared the content, having particular regard to the importance of minimising the reporting of **false positives** to the National Crime Agency (NCA) or a foreign agency.

ICU PT 1.14 The incorporating feedback criterion is fulfilled if feedback and quality assurance mechanisms are in place to maintain or improve performance of the **relevant technology** and **associated systems and processes** over time.

This includes:

a) identifying, correcting and responding to errors and performance issues,
b) updating the **relevant technology** with diverse and up-to-date datasets to reflect evolving trends or emerging types of **image-based CSAM content**, and
c) integrating ongoing feedback from users and individuals working in moderation into its development, while managing the risk of introducing additional bias.

ICU PT 1.15 For the purposes of ICU PT 1.3, the provider should have regard to at least the **risk assessment** of the service, including:

a) the particular needs of its ***United Kingdom user*** base as identified in its **risk assessment**, including relevant languages used on the service; and
b) how **image-based CSAM** manifests on the service.

ICU PT 1.16 For the purposes of ICU PT 1.3, the provider should ensure that **relevant inputs** that are generated on, uploaded to or shared on the service (or that a ***user*** seeks to so generate, upload or share) after the **relevant technology** is implemented are analysed before, or as soon as practicable after, **relevant content** can be ***encountered*** by ***United Kingdom users*** of the service.

ICU PT 1.17 For the purposes of ICU PT 1.3, the provider should ensure that all **relevant content** present on the service when the technology is first implemented is analysed within a reasonable time.

ICU PT 1.18 When deploying **text matching technologies**, the provider should treat detection by the technology as reason to suspect that items of content associated with the matched text may be ***illegal content*** and review that content in accordance with Recommendation ICU C1.3 of the Illegal content Codes of Practice for user-to-user services.

ICU PT 1.19 When deploying **application-specific machine learning technologies** the provider should treat detection by the technology as reason to suspect that the content may be ***illegal content*** and review the content in accordance with Recommendation ICU C1.3 of the Illegal content Codes of Practice for user-to-user services.

ICU PT 1.20 The provider should maintain sufficient records to demonstrate the basis on which it concluded the **relevant technology** met the **proactive technology criteria**, including records of any testing or evaluation undertaken, the performance metrics used, the results obtained, configuration decisions, identified limitations and mitigations, and any ongoing monitoring and review activities relevant to its assessment.

ICU PT 1.21 At least every 12 months, or earlier where there is a change to any aspect of the service's design or operation which would amount to a significant change and therefore trigger a risk assessment under section 9(4) of the **Act**, the provider should review its selection of **relevant technology**.

ICU PT 1.22 This recommendation is separate to, and does not affect, Recommendations ICU C9 (using hash matching to detect and remove CSAM) and ICU C10 (detecting and removing content matching listed CSAM URLs) of the Illegal content Codes of Practice for user-to-user services.

Safeguards for freedom of expression and privacy

ICU PT 1.23 Paragraphs ICU PT 1.4-1.21 of this Recommendation ICU PT 1 are safeguards to protect ***United Kingdom users'*** right to freedom of expression and the privacy of ***United Kingdom users***.

ICU PT 1.24 The following measures in the Illegal content Codes of Practice for user-to-user services 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 C4.A, ICU C5, 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 **content 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 D7 and ICU D8 or ICU D9 (whichever is applicable), ICU D10 (in relation to **content appeals**), ICU D11 and ICU D12; and
d) Recommendation ICU G1 (terms of service: substance (all services)).

5. Definitions and interpretation

5.1 Terms in bold used in this Code have the meanings set out in table A. The meaning given applies even if the term is also used in the Act.

5.2 Terms in bold and italics used in this Code have the same meaning as in the Act. Table B provides a reference to the provision(s) in the Act containing the definition of the relevant term as well as additional notes and references which are intended to assist the reader. In the event of any inconsistency between the Act and the information in table B, the Act should be regarded as authoritative.

5.3 Terms which are underlined are references to kinds of illegal harms set out in table C.

Table A - Definitions of terms in bold used in these Codes

Term	Meaning
Act	The Online Safety Act 2023 (c.50).
Active United Kingdom user	As defined in paragraph 5.10.
Application-specific machine learning technologies	Technologies based on models developed or adapted using training data to identify, classify, or assess features, attributes, or characteristics of **target content**, and whose intended tasks, decision criteria, and expected outputs are established through model development or adaptation.
Associated systems and processes	The ***systems and/or processes*** associated with the use of ***proactive technology***.
Content appeal	A complaint by a ***United Kingdom user*** about any of the following actions, if the action concerned has been taken by the ***provider*** on the basis that ***content*** generated, uploaded or shared by that user is ***illegal content****:* a) the content being taken down; b) the user being given a warning; c) the user being suspended, banned, or in any other way restricted from using the **service**.

Term	Meaning
CSAM (child sexual abuse material)	***Content*** that amounts to an offence specified in any of the following paragraphs of Schedule 6 to the **Act**— a) paragraph 1 to 4, 7 or 8; b) paragraph 9 so far as any of the offences it contains are committed in relation to an offence specified in paragraphs 1 to 4, 7 or 8; c) paragraph 10; or d) paragraph 13 so far as any of the offences it contains are committed in relation to an offence specified in paragraph 10. Where the context requires, references to CSAM include material which would be CSAM if it were ***regulated user-generated content*** present on a **service**.
Detect	To identify ***content*** as being (or as likely to be) **target content**.
Detected content	***Content*** detected by the use of **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.**
File-storage and file-sharing service	A **service** whose primary functionalities involve enabling ***users*** to: a) store digital content, including images and videos, on the cloud or dedicated server(s); and b) share access to that content through the provision of links (such as unique **URLs** or hyperlinks) that lead directly to the content for the purpose of enabling other ***users*** to ***encounter*** or interact with the content.
Image-based CSAM content	***Content*** amounting to an offence specified in any of the following paragraphs of Schedule 6 to the **Act**: 2 to 4, 7 or 10, so far as the risk in relation to those offences relates to **CSAM** in the form of photographs, videos or visual images.
Large service	A **service** which has more than 7 million monthly **active United Kingdom users** (see paragraphs 5.6 to 5.9).
Precision	A measure of statistical accuracy, calculated as the proportion of **detected content** that a **relevant technology** has correctly identified as **target content**.
Proactive technology criteria	As defined in ICU PT 1.4.

Term	Meaning
Recall	A measure of statistical accuracy, calculated as the proportion of **target content** analysed by a **relevant technology** that the technology has **detected**.
Regulated user-to-user service	A ***user-to-user service*** as defined in section 3 of the **Act**, which is a regulated user-to-user service under section 4 of the **Act** (subject to the disapplication in section 5 of the **Act**).
Relevant content	Any: a) ***regulated user-generated content*** that: i) may be ***encountered*** by ***United Kingdom users*** of the service by means of the service, and ii) is communicated publicly [2] by means of the service, or b) material which, if it were present on the service, would be content within paragraph (a).
Relevant inputs	**Relevant content** or metadata relating to **relevant content**.
Relevant technology	A form of ***proactive technology*** that constitutes one or a combination of the specified technologies for the purposes of ICU PT 1 and has been implemented by a ***provider*** to **detect target content**.
Risk	See the subsection headed 'Risks of illegal harm' below (which begins at paragraph 5.4).
Risk assessment	The most recent risk assessment carried out by the ***provider*** pursuant to section 9 of the **Act**.
Service	A **regulated user-to-user service**.
Target content	**Image-based CSAM content**.
Text matching technologies	Exact matching, approximate matching, or pattern matching technologies based on rule-based or heuristic matching approaches to identify predefined textual elements and patterns within content, including words, phrases, character sequences, uniform resource locators (URLs), and domain names.
Undetected content	**Relevant content** that was not **detected** by the ***relevant technology*** and was brought to the attention of the ***provider*** as being suspected **target content** by another means.

[2] Ofcom has published guidance on content communicated 'publicly' and 'privately' under the Online Safety Act for this purpose.

Term	Meaning
Unknown image-based CSAM content	**Image-based CSAM content** that is not included in any reference database of hash values for **CSAM** used by the provider in order to comply with ICU C9 of the Illegal content Codes of Practice for user-to-user services.

Table B - Terms used in these Codes that have the meaning given in the Act

Term	Meaning under the OSA
Affected person	Section 20(5) See also section 21(7).
Content	Section 236(1) See the entry for "internet service" regarding the definition of that term. See section 232 in relation to "content communicated "publicly" or "privately".
Content identification technology	Section 231(2) Under section 231(1), content identification technology is listed as a form of "proactive technology". Section 231(3) describes situations where content identification technology will not be proactive technology.
Encounter (in relation to content)	Section 236(1)
Illegal content	Section 59(2) Section 59(3) sets out when content will amount to a relevant offence. Sections 59(4), (5) and (7) set out what is meant by a relevant offence. Section 59(6) describes offences which are not relevant offences. Sections 59(11) to (15) contain further interpretative provisions. See the entries for "content" and "regulated user-generated content" regarding the definitions of those terms. A "regulated user-to-user service" is a "user-to-user service" (see the entry for "user-to-user service" regarding the definition of that term) which is a regulated user-to-user service under section 4 (subject to the disapplication in section 5).
Internet service	Section 228(1) and section 204(1) Sections 228(2) and (3) describe what is meant by a service that is made available by means of the internet.

Proactive technology	**Section 231(1)** Sections 231 (4) and (6) define "user profiling technology" and "behaviour identification technology". Sections 231(3), (5) and (7) explain when these technologies will not be proactive technology. Sections 231(8) to (13) contain further interpretative provisions. See the entries for "content", "content identification technology", "illegal content", "internet service", "user", "user-generated content" and "user-to-user service" regarding the definition of those terms. Section 236(1) defines "personal data". Section 4(4) defines "regulated service". A "regulated user-to-user service" is a "user-to-user service" (see the entry for "user-to-user service" regarding the definition of that term) which is a regulated user-to-user service under section 4 (subject to the disapplication in section 5).
Provider	**Section 226** See the entries for "internet service" and "user" regarding the definition of those terms.
Regulated user-generated content	**Section 55(2)** Sections 55(5) to (12) contain interpretative provisions. A "regulated user-to-user service" is a "user-to-user service" (see the entry for "user-to-user service" regarding the definition of that term) which is a regulated user-to-user service under section 4 (subject to the disapplication in section 5). See the entries for "content", "user" and "user-generated content" regarding the definitions of those terms. Section 236(1) defines "identifying content". Section 56 defines "recognised news publisher".
Systems and/or processes	**Section 236(1)**
United Kingdom user	**Section 227(1)** See the entry for "user" regarding the definition of that term.
User	**Section 227(2)-(3)** Section 227(3) sets out individuals and entities that will not be users for the purposes of the Act. Sections 227(4) to (6) provide

	further interpretation of terminology used throughout section 227. See the entries for "internet service" and "user-to-user service" regarding the definitions of those terms. Sections 228(2) and (3) describe what is meant by a service that is made available by means of the internet.
User-generated content	**Section 55(3) and (4)** See the entries for "user" and "user-to-user service" regarding the definitions of those terms. Section 55(4) provides interpretation of the scope of "content generated, uploaded or shared by a user" and explains when a bot or other automated tool may be regarded as a user of a service.
User-to-user part (of a service)	**Section 236(1)** See the entries for "user-generated content" and "user-to-user service" regarding the definitions of those terms.
User-to-user service	**Section 3(1) and (2)** and **section 204(1)** See the entries for "content", "encounter", "internet service" and "user" regarding the definitions of those terms.

Risks of illegal harm

Risk of a kind of illegal harm

5.4 A service is at medium or high risk of a kind of illegal harm set out in table C if either:

a) the **risk assessment** of the service identified a medium or high risk [3] (as the case may be) in relation to the offences (taken together) as specified in relation to that kind of harm in table C; or

b) by virtue of a confirmation decision given under section 134 of the **Act** in relation to a risk of serious harm, the duty set out in section 10(2)(b) or (c) of the **Act** applies in relation to the service as if an illegal content risk assessment carried out by the provider pursuant to section 9 of the **Act** had identified a medium or high risk of serious harm (as the case may be) in relation to that kind of harm.

5.5 In relation to the offence specified in table C, the offence also, to the extent relevant, includes the offences of encouraging, assisting, conspiring to commit, aiding, abetting, counselling, procuring, attempting, or (in Scotland) inciting or being involved art and part in, the commission of that offence.

[3] Ofcom has given guidance on risk assessments entitled 'Risk Assessment Guidance and Risk Profiles' (16 December 2024).

Table C - Kinds of harm

	Term	Meaning
1.	***Image-based CSAM***	An offence specified in any of paragraphs 1 to 4, 7, 8 or 10 of Schedule 6 to the **Act**, so far as the risk in relation to those offences relates to **CSAM** in the form of photographs, videos or visual images.

User numbers

5.6 This subsection applies for the purpose of determining whether a **service** has more than a particular number of monthly **active United Kingdom users**.

5.7 A **service** has more than a particular number of monthly **active United Kingdom users**:

a) from such time as the average number of monthly **active United Kingdom users** is more than that number; and
b) until such time as the average number of monthly **active United Kingdom users** has been at or below that number for a continuous period of six months.

5.8 A **service's** average number of monthly **active United Kingdom users** is the mean number of **active United Kingdom users** per month for:

a) the six-month period ending with the month preceding the time in question; or
b) where the **service** has been in operation for less than six months, the period for which the service has been in operation.

5.9 In this subsection, an **active United Kingdom user** means any **United Kingdom user** who has accessed the **user-to-user** part of the service.

E03719696

978-1-5286-6893-4