STATUTORY INSTRUMENTS

2026 No. 268

ELECTRONIC COMMUNICATIONS

The Online Safety (CSEA Content Reporting by Regulated User-to-User Service Providers) Regulations 2026

Made - - - -	*9th March 2026*
Laid before Parliament	*12th March 2026*
Coming into force - -	*7th April 2026*

The Secretary of State makes these Regulations in exercise of the powers conferred by sections 67 and 224(1)(a)(i) of the Online Safety Act 2023(**a**).

The Secretary of State has consulted the National Crime Agency and the Office of Communications and such other persons as the Secretary of State has considered appropriate as required by section 67(5) of that Act.

Citation, commencement and extent

1.—(1) These Regulations may be cited as the Online Safety (CSEA Content Reporting by Regulated User-to-User Service Providers) Regulations 2026.

(2) These Regulations come into force on 7th April 2026.

(3) These Regulations extend to England and Wales, Scotland and Northern Ireland.

Interpretation

2. In these Regulations—

"the Act" means the Online Safety Act 2023;

"API" means an application programming interface which can be used to submit reports of CSEA content to the NCA(**b**);

"connections with other accounts" means connections created as a result of a provider's service functionality that allow users to establish a direct link between two user accounts;

"CSEA content" has the meaning given in section 59 of the Act;

(**a**) 2023 c. 50.
(**b**) "NCA" has the meaning given in section 70(7) of the Act.

"data protection legislation" has the meaning given in section 3(9) of the Data Protection Act 2018(**a**);

"exif data"—

(a) means metadata embedded within a digital image or video file created in accordance with the exchangeable image file format standard, and

(b) includes information relating to the circumstances of the file's creation, such as the date and time of capture, device identifiers, technical camera settings and, where applicable, geolocation co-ordinates;

"hash value" means a string of characters generated by applying mathematical algorithms to a digital file which uniquely represents the content of that file, such as an image or video;

"IP address" means the internet protocol address of a device;

"online portal" means the online portal managed by the NCA which has been provided for the purpose of enabling an organisation administrator or an authorised person to send reports of CSEA content to the NCA;

"platform" means a user-to-user part of a user-to-user service(**b**);

"port number" means a connection endpoint;

"provider" means a UK provider(**c**) of a regulated user-to-user service(**d**), or a non-UK provider(**e**) of a regulated user-to-user service;

"registering party" means the provider or the third party provider who is registering prescribed information with the NCA;

"reporting duty" means the requirement under section 66 of the Act on providers to report detected(**f**) and unreported(**g**) CSEA content to the NCA;

"reporting person" means the person who is submitting a manual report through the online portal, or the person who is the point of contact for reports submitted using the API;

"senior manager" means an individual who plays a significant role in making decisions about, managing or organising the registering party's activities in relation to the reporting duty, and who could reasonably be expected to ensure compliance;

"third party provider" means a person with whom the provider has contracted to carry out its reporting duty;

"URL" means the full universal resource locator.

(**a**) 2018 c. 12; section 3(9) was amended by S.I. 2019/419, Schedule 2, paragraph 4(3) and The Data (Use and Access) Act 2025 (c. 18), section 107(2) and Schedule 11, paragraph 14.
(**b**) "User-to-user service" has the meaning given in section 3 of the Act.
(**c**) "UK provider" has the meaning given in section 70(2) of the Act.
(**d**) "Regulated user-to-user" service has the meaning given in section 4(2) of the Act.
(**e**) "Non-UK provider" has the meaning given in section 70(3) of the Act.
(**f**) "Detected" has the meaning given in section 70(4) of the Act.
(**g**) "Unreported" has the meaning given in section 70(5) of the Act.

Reporting duty

3.—(1) A provider may arrange for a third party provider to carry out the reporting duty on its behalf.

(2) Where a provider makes an arrangement with a third party provider to carry out the reporting duty on its behalf, the provider must notify the NCA as soon as reasonably practicable that it has done so.

(3) Where a provider uses a third party provider and the arrangement ceases, the provider must notify the NCA as soon as reasonably practicable that the arrangement has ceased.

(4) Where a provider which has registered with the NCA in accordance with regulation 4 is required or decides to report CSEA content to a foreign agency(**a**) instead, it must as soon as reasonably practicable—

(a) notify the NCA that it will report CSEA content to a foreign agency, and

(b) cease to report CSEA content to the NCA.

Registration with the NCA

4.—(1) A provider and any third party provider must register with the NCA prior to submitting their first report pursuant to the reporting duty.

(2) The registering party must provide the following information to the NCA by using the online portal—

(a) name of the registering party,

(b) business address of the registering party, and

(c) country in which the registering party is based.

(3) The registering party must also register the relevant contact details listed in paragraph (5) with the NCA by using the online portal.

(4) Where a provider is using the services of a third party provider, both the provider and the third party provider must register the relevant contact details listed in paragraph (5).

(5) The relevant contact details are the name, email address and telephone number (including an international dialling code) of—

(a) the organisation administrator,

(b) the deputy organisation administrator, if appointed,

(c) an emergency contact (who may be the same person as the organisation administrator or deputy organisation administrator), and

(d) each authorised person.

(6) The registering party must keep those relevant contact details up to date for the duration of the reporting activity carried out under these Regulations.

The organisation administrator, deputy organisation administrator, and authorised persons

5.—(1) The registering party must—

(a) appoint a person to act as the main point of contact with the NCA (the "organisation administrator"), and

(**a**) "Foreign agency" has the meaning given in section 70(7) of the Act.

(b) appoint a replacement organisation administrator in the event that the person appointed under sub-paragraph (a) ceases to act in that capacity.

(2) The organisation administrator must be a senior manager or other individual whom the registering party considers has an equivalent appropriate role in the organisation.

(3) An organisation administrator may appoint an authorised person to be deputy organisation administrator.

(4) An organisation administrator or deputy organisation administrator may authorise one or more individuals within their organisation to report CSEA content to the NCA (each one is "an authorised person").

(5) The provider and any third party provider must ensure that an authorised person does not share their login details to the online portal with any other person.

(6) Where an API is used to submit reports—

(a) the organisation administrator or deputy organisation administrator must be responsible for configuring and establishing the API process, and

(b) the registering party must provide a point of contact for reports submitted using the API.

Making reports to the NCA

6.—(1) Where the reporting duty applies, a report must be sent by the provider or the third party provider to the NCA, in accordance with the time frames set out in paragraph (7).

(2) Where a report is sent to the NCA, it must be submitted through the online portal or using an API.

(3) Reports submitted through the online portal may only be sent by an organisation administrator, a deputy organisation administrator or any other authorised person.

(4) The report—

(a) must contain the information set out in Schedule 1 (where that information is available),

(b) must contain an indication of priority level, as defined in paragraph (6),

(c) must comply with the formatting requirements set out in Schedule 2, and

(d) may contain any other available information that is relevant to the incident of CSEA content.

(5) Where any information required by Schedule 1 is not available at the time the report is to be made, an initial report must be made containing the information which is available, followed by a supplementary report as soon as other information becomes available.

(6) The criteria for assessing priority levels are—

(a) Priority level 1: where there is information which suggests that there is an immediate threat to a child's life, or immediate risk of serious harm to a child;

(b) Priority level 2: where there is information which suggests that there could be a risk of serious harm to a child in the near future, or that urgent safeguarding of a child might be required;

(c) Priority level 3: where the criteria for priority level 1 or 2 are not reached.

(7) The time frames for sending reports are—

(a) for priority level 1, immediately;

(b) for priority level 2, as soon as reasonably practicable;

(c) for priority level 3, without undue delay.

Requests from the NCA

7. Where the NCA makes a request to the registering party for information about itself or a report, the registering party must respond as soon as reasonably practicable and, in any event, within 7 days.

Retention of data

8.—(1) Where a report has been sent to the NCA in accordance with regulation 6(1), the provider must retain—

(a) for a period of five years from the date of issue, the unique report reference number (which appears on the automated receipt), and

(b) for a period of one year—

(i) the detected CSEA content,

(ii) the information submitted in accordance with these Regulations,

(iii) any information which has been used to make a judgement that the content is CSEA content, and

(iv) any relevant data associated with the user who uploaded, created, shared or received the CSEA content,

beginning with the date on which the report was sent.

(2) For the purposes of paragraph 1(b)(iv), relevant data is any of the following data from the two-week period prior to the CSEA content being uploaded, created, shared or received—

(a) any digital files with content which the user has uploaded, created, shared or received on the internet service,

(b) any digital files with metadata or communications data associated with the CSEA content,

(c) any digital files with geolocation data in addition to that included in the metadata,

(d) any digital files with chat logs, public and private messages, and public comments created by the user, and

(e) any digital files with information about connections with other accounts (including attempted connections).

Data protection requirements

9. Where data protection legislation does not apply, the provider, when processing personal data in compliance with these Regulations must take steps to ensure appropriate security and confidentiality of the data.

Jess Phillips
Parliamentary Under-Secretary of State
Home Office

9th March 2026

SCHEDULE 1

Regulation 6(4)(a)

Information to be included in reports

1. Contact information about the reporting person—

(a) name,

(b) email address, and

(c) telephone number (including an international dialling code).

2. The detected CSEA content.

3. Information about the detected CSEA content—

(a) method by which it was detected,

(b) platform on which it was detected,

(c) whether the report relates to a previous report,

(d) if the report relates to a previous report, the unique reference number of the previous report,

(e) time at which it was uploaded,

(f) date on which it was uploaded,

(g) IP address of the device the file was uploaded from and any port number associated with that IP address,

(h) date and time associated with the IP address mentioned in (g) above,

(i) exif data linked to it,

(j) URL of the webpage on which it was uploaded, and

(k) its original hash value.

4. Information about the user who has uploaded, created, shared or received the CSEA content—

(a) account username,

(b) name, address and date of birth listed on the billing details,

(c) email address,

(d) recovery email address,

(e) telephone number (including an international dialling code),

(f) confirmation of whether the user's telephone number has been verified and, if so, the date on which it was verified,

(g) URL of the user's profile on the platform where the CSEA content was detected, and

(h) the registration and login IP addresses for the user's account during the three months prior to the report being made, and the time, date and any port number connected with those IP addresses.

5. A declaration that all the available information has been provided.

SCHEDULE 2

Regulation 6(4)(c)

Formatting requirements

1. Dates must be provided in number format as DD/MM/YYYY.

2. Time must be provided in an international format and the person making the report must select the appropriate time zone for the time recorded by the system.

3. IP addresses must be formatted as follows—

(a) in the case of an IPv4 address, as four sets of numbers separated by dots, and

(b) in the case of an IPv6 address, as eight groups of four hexadecimal digits separated by colons.

EXPLANATORY NOTE

(This note is not part of the Regulations)

Section 66 of the Online Safety Act 2023 (c. 50) requires certain providers of regulated user-to-user services to report child sexual abuse and exploitation content ("CSEA content") detected on their internet service to the National Crime Agency ("NCA"). If these providers already have arrangements in place for reporting CSEA content to a foreign agency which is exercising functions similar to the NCA (such as the National Center for Missing & Exploited Children in the United States of America), then this content is not required by section 66 to be reported to the NCA.

Where a provider must report CSEA content to the NCA, regulation 4 requires them to register with the NCA before they do so. Where those providers have entered into arrangements with another person to carry out the reporting duty on their behalf, that person is also required to register with the NCA.

Regulation 6 requires certain information to be included in the reports made to the NCA. The Regulations specify the manner in which reports of CSEA content must be sent to the NCA and the format in which these reports must be sent. The Regulations also require providers to assess the urgency of the report and to send the report to the NCA in accordance with certain time frames depending on their assessment of urgency.

Regulation 8 requires providers to retain records of reports made to the NCA, and to retain certain information about the users who are associated with a report.

Schedule 1 to these Regulations sets out the information required to be included in the reports to the NCA. Schedule 2 contains formatting requirements for the reports.

A full impact assessment has been published in relation to the Online Safety Act 2023 and copies can be obtained from the UK Government website at: https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf or from the Department for Science, Innovation and Technology at 100 Parliament Street, London SW1A 2BQ, United Kingdom.

© Crown Copyright 2026

Printed and published in the UK by The Stationery Office Limited under the authority and superintendence of Saul Nassé, Controller of His Majesty's Stationery Office and King's Printer of Acts of Parliament.

ISBN 978-0-34-828090-6

£8.90

http://www.legislation.gov.uk/id/uksi/2026/268