Protecting people from illegal harms online

Record-Keeping and Review Guidance

Guidance

Published 16 December 2024

Contents

1. Introduction

1.1 Under the Online Safety Act 2023 (the Act), providers of regulated user-to-user (U2U) services and regulated search services are required to keep records of their risk assessments and the measures taken to comply with some of the new duties and to review them regularly. This guidance is intended to assist providers with doing so.

Who does this guidance apply to?

1.2 This guidance applies to providers of regulated U2U services and regulated search services (service providers).

What does this guidance cover?

1.3 This guidance covers the duties on service providers that are set out in sections 23 and 34 of the Act.[1] These comprise:

a) the 'record-keeping duties', namely the duties to:

i) keep written records of their risk assessments;
ii) keep written records of measures taken as described in a Code of Practice to comply with a relevant duty;[2]
iii) where the measure described in a Code of Practice has not been taken, keep a written record of the alternative measure taken and how that fulfils the relevant duty; and

b) the 'review duties', namely the duties to:

i) review compliance with the relevant online safety duties regularly;[3] and
ii) review compliance with the relevant online safety duties as soon as practicable after making a significant change to the design or operation of the service.

---

[1] This guidance does not cover the record-keeping duties that apply to providers which provide an online service on which pornographic content is published or displayed by or on behalf of that provider ('Part 5 providers'). Guidance on those duties is included in our draft Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services, which we published in December 2023. This guidance also does not cover guidance on written records for children's access assessments (conducted under section 36) or children's risk assessments (carried out under section 11 or section 28 of the Act). This is included in our draft Children's Access Assessments or draft Children's Risk Assessment Guidance, which we published in May 2024.

[2] A 'relevant duty' for regulated U2U services means the duties set out in: section 10 (illegal content); section 12 (children's online safety); section 15 (user empowerment); section 17 (content of democratic importance); section 19 (journalistic content); section 20 (content reporting); and section 21 (complaints procedures). A 'relevant duty' for regulated search services means the duties set out in: section 27 (illegal content); section 29 (children's online safety); section 31 (content reporting); and section 32 (complaints procedures).

[3] For regulated U2U services, these are the duties set out in: section 10 (illegal content); section 12 (children's online safety); section 15 (user empowerment); section 17 (content of democratic importance); section 18 (news publisher content); section 19 (journalistic content); section 20 (content reporting); section 21 (complaints procedures); section 71 and section 72 (terms of service); and section 75 (disclosure of information about use of service by deceased child users). For regulated search services, these are the duties set out in: section 27 (illegal content); section 29 (children's online safety); section 31 (content reporting); section 32 (complaints procedures); and section 75 (disclosure of information about use of service by deceased child users).

1.4 Our guidance also references the duties on service providers of Category 1 U2U services and Category 2A search services to provide the written records of their risk assessments to Ofcom.[4]

1.5 For duties relating to illegal content, this guidance should be read alongside the Illegal Content Codes of Practice and our guidance on illegal content risk assessments (Risk Assessment Guidance and Risk Profiles).[5]

Why is this guidance important?

1.6 This guidance is designed to help service providers understand what is expected in relation to keeping written records of risk assessments and the measures taken to comply with the relevant duties and reviewing compliance with the relevant duties.

1.7 Well-maintained, clear records, and regular, timely reviews will assist service providers to keep track of compliance with the relevant duties and ensure that the measures taken are fit for purpose. The records will also provide a useful resource for Ofcom in monitoring how the relevant duties are being fulfilled.

Failure to keep records or review compliance

1.8 The record-keeping and review duties are enforceable by Ofcom. When considering whether a service provider has complied with the duties, we will take into account whether it has acted in accordance with this guidance. Any enforcement action will be taken in line with the procedures set out in our Online Safety Enforcement Guidance.[6]

1.9 If we find a service provider to be in breach of these duties, we have the power to fine service providers up to £18 million or 10% of qualifying worldwide revenue, whichever is the greater.

[4] Section 23(10) and section 34(9) respectively of the Act. Category 1 U2U services and Category 2A search services are services that Ofcom considers meet the applicable threshold conditions set out in regulations to be made by the Secretary of State under Schedule 11 of the Act and that are entered in a public register to be kept by Ofcom under section 95 of the Act.

[5] See our regulatory documents: Illegal Content Codes of Practice for U2U services; Illegal Content Codes of Practice for search services; and Risk Assessment Guidance and Risk Profiles.

[6] Online Safety Enforcement Guidance.

2. Guidance on written records

2.1 To comply with the record-keeping duties, service providers must make and keep written records which should be durable, accessible, easy to understand, and up to date.

Durability and accessibility

2.2 Written records should be made and kept in a durable medium of the provider's choice (for example, on a computer or using any storage device such as a CD-ROM, USB memory stick, cloud storage, a network drive, or a paper copy), which is capable of being provided easily and quickly to Ofcom if required.

Easy to understand

2.3 Written records should be legible and written in as simple and clear language as possible. They should not include jargon, encryption, shorthand, or code such that Ofcom cannot understand what they say.

2.4 Where reasonably practicable, written records should be kept in English (or for service providers based in Wales, in English or Welsh). If this is not reasonably practicable, it should be possible for an English translation of records to be provided.

Up to date

2.5 A written record must be kept of current risk assessments and any measures taken to comply with a relevant duty. While the record must be updated to capture changes made to the risk assessment or measure in question, it is important that earlier versions of the record are retained so that the provider is able to provide both current and historic records of how it has complied with the relevant duties.[7]

2.6 Unless the record in question has been provided to Ofcom, written records that are no longer current should be retained in accordance with the service provider's record retention policies, or a minimum of **three years** (either calendar or financial), whichever is longer.

2.7 The written record should be dated when it is made and on each occasion that it is updated.[8]

[7] See paragraphs 6.1 to 6.8 for guidance on the service provider's duty to conduct a review of a measure when there has been a significant change to any aspect of the design or operation of a regulated service.
[8] We set out in paragraphs 3.13, 4.5, and 5.6 when the respective written records should be made.

3. Making and keeping written records of risk assessments

What must service providers do?

All service providers

3.1 Service providers are required to make and keep a written record, in easily understandable form, for all aspects of every illegal content risk assessment.[9]

3.2 The record should include details of how the risk assessment was carried out and its findings, including:

a) how a service provider has consulted Ofcom's Risk Profiles;[10]
b) the evidence used to assess risks; and,
c) the outcomes of the risk assessment.

3.3 The record should help to demonstrate that a provider's risk assessment is suitable and sufficient. It should include how the provider has considered the required elements in section 9 or section 26 (as applicable) of the Act and the evidence the provider has relied on to assess the risks relevant to the provider's service.

Category 1 U2U services and Category 2A search services

3.4 Ofcom will publish a register of categorised services.[11] The providers of the services that are categorised as Category 1 U2U services and Category 2A search services will have certain additional duties, including the duty to provide risk assessments to Ofcom and the duty to publicly summarise the findings of the most recent risk assessment.

Duty to provide risk assessments to Ofcom

3.5 As soon as reasonably practicable after making or revising a written record of an illegal content or a children's risk assessment, Category 1 U2U service providers and Category 2A search service providers are required to provide this written record (in full) to Ofcom.[12] The record should be sent to Ofcom in electronic format to the dedicated Ofcom email address, as published on Ofcom's website at the time of submission.

3.6 We anticipate that a service provider will make a record of its risk assessment as it is being carried out, so the provider should be able to send the record to Ofcom as soon as the risk assessment, or revision to it, is concluded.

[9] Section 9 and section 26 of the Act as applicable.
[10] All providers must take account of the relevant Risk Profiles for their service when conducting the risk assessment. There is a separate set of risks for U2U services and for search services. The Risk Profiles are available in our Risk Assessment Guidance and Risk Profiles published document.
[11] Categorised services are services that Ofcom considers meet the applicable threshold conditions set out in regulations to be made by the Secretary of State under Schedule 11 of the Act and that are entered in a public register to be kept by Ofcom under section 95 of the Act.
[12] Section 23(10) and section 34(9) of the Act respectively.

Duty to publicly summarise the findings of the most recent risk assessment

3.7 Providers of Category 1 U2U services must summarise in their terms of service the findings of the most recent risk assessment of their service (including levels of risk, and the nature and severity of potential harm to individuals).[13]

3.8 Providers of Category 2A search services must summarise in a publicly available statement the findings of their most recent risk assessment (including levels of risk, and the nature and severity of potential harm to individuals).[14]

What should the risk assessment record include?

3.9 A regulated provider's record of its risk assessment must provide details about how it was carried out and its findings.

3.10 The record should include the following information:

a) the service to which the risk assessment relates;
b) the date the risk assessment was completed;
c) if applicable, the date the risk assessment was reviewed or updated;
d) who completed the risk assessment, and the named person responsible for the risk assessment; and
e) who approved the risk assessment.

3.11 A record of an illegal content risk assessment should also include the following information regarding how a service provider has undertaken the risk assessment, and its findings:

a) confirmation that a service provider has consulted Ofcom's Risk Profiles. A service provider may do this by recording the outcomes of the Risk Profiles questionnaire in Part 3 Section 1 of the Risk Assessment Guidance and Risk Profiles document;[15]
b) a record of any risk factors from Ofcom's Risk Profiles that are relevant to the regulated provider's service;
c) if applicable, a list of any additional characteristics (including user base, business models, functionalities, governance, and systems and processes) the regulated provider has considered alongside the risk factors identified in Ofcom's Risk Profiles;
d) where a service provider has considered the role of any existing controls already in operation on the service at the time of the risk assessment, what these controls are, what risks they are intended to mitigate and how they do this, and how the consideration of the existing controls has impacted the risk level assigned by the provider to a kind of illegal content;
e) the level of risk (high, medium, low, negligible) assigned to each of the 17 kinds of priority illegal content (and, for U2U services, a risk level for each kind of CSAM) and any relevant other illegal content, and an evidence-based explanation of the decision. Where appropriate, this should also include the level of risk assigned to sub-categories of harm (including image-based CSAM, CSAM URLs, and Grooming);
f) a list of the evidence, and summary of the reasoning, that has informed the assessment of likelihood and impact of each of the 17 kinds of priority illegal content and any relevant other illegal content;

[13] Section 10(9) or section 12(14) of the Act, as applicable.
[14] Section 27(9) or 29(9) of the Act, as appliable.
[15] Risk Assessment Guidance and Risk Profiles.

g) confirmation that the findings of the risk assessment have been reported, and recorded, through appropriate governance channels; and
h) information regarding how a service provider takes appropriate steps to keep the risk assessment up to date (for example, a written policy).

3.12 Providers should refer to the Risk Assessment Guidance and Risk Profiles regulatory document for more detailed guidance on how to carry out an illegal content risk assessment.[16]

When should the risk assessment record be made?

3.13 The written record of the risk assessment (or a revision to the risk assessment) should be made contemporaneously to ensure it is accurate and up to date.

[16] See Risk Assessment Guidance and Risk Profiles.

4. Records of measures taken in compliance with a relevant duty which are recommended in Ofcom's Code of Practice

What must service providers do?

4.1 Where the service provider adopts measures set out in Ofcom's Code of Practice for the purpose of compliance with one or more of the relevant duties set out in Table 1, the provider should keep a written record of the measures taken.

Table 1: relevant duties for service providers:

'Relevant duties' for regulated U2U services	'Relevant duties' for regulated search services
a) illegal content (section 10) b) children's online safety (section 12) c) user empowerment (section 15) d) content of democratic importance (section 17) e) journalistic content (section 19) f) content reporting (section 20) g) complaints procedures (section 21)	a) illegal content (section 27) b) children's online safety (section 29) c) content reporting (section 31) d) complaints procedures (section 32)

What should the record include?

4.2 There should be a written record of each measure that is taken or is in use as described in the Code of Practice, which:

a) provides a description of the measure in question;
b) identifies the relevant Code of Practice; and
c) gives the date that the measure takes effect.

4.3 To help service providers record this information, for each of the measures Ofcom recommends, we set out which duty it relates to in the relevant Code of Practice.

4.4 Where a measure in a Code of Practice provides for a document to be made or information to be recorded (such as a written policy or statistical records), the document or information

in question (or a copy) should be kept and maintained as part of the record made for the purposes of the record-keeping duty under section 23(3) or section 34(3).[17]

When should the record of a Code measure be made?

4.5 The written record of a Code measure should be made promptly. Where the measure is already in effect prior to the relevant duty coming into force, the written record should be made promptly after the duty has come into effect.

[17] Such document or information should be durable, accessible, easy to understand, and up to date, in line with this guidance.

5. Records of alternative measures taken to comply with a relevant duty

What must service providers do?

5.1 Codes of Practice describe the measures that Ofcom recommends service providers take to comply with the relevant duties to which the Code of Practice applies. However, a service provider has the option of taking alternative measures to those set out a Code of Practice to comply with a relevant duty.

5.2 If a service provider adopts, or has already adopted, alternative measures to those set out in the Code of Practice to comply with its relevant duties (see Table 1) then it must make and keep a written record of the alternative measures.

What should the record of an alternative measure include?

5.3 Written records must include:

a) the measures in a Code of Practice that have been recommended based on the outcome of the risk assessment but have not been taken or are not in use;[18] [19]
b) the alternative measures that have been taken or are in use;
c) how those alternative measures amount to compliance with the duty in question; and
d) how the provider has complied with section 49(5) (freedom of expression and privacy).

5.4 Where service providers adopt alternative measures to comply with the safety duties in relation to illegal content, or the safety duties protecting children, the written record must also state whether the alternative measures have been taken or are in use in every area listed in Table 2 (to the extent there are applicable measures in a Code of Practice).[20] [21]

[18] These are measures set out by Ofcom in a Code of Practice which apply to the relevant service provider.
[19] There is no obligation on a service provider to keep a written record of a measure (from the Code of Practice) that does not apply to it (for example, where particular measures only apply to a subset of services based on size or risk of a particular harm).
[20] Specifically, the duties in section 10(2) and (3) for U2U services and section 27(2) and (3) for search services in relation to safety duties about illegal content; and the duties in section 12(2) and (3) for U2U services and section 29(2) and (3) for search services in relation to safety duties protecting children.
[21] See section 23(5) and section 34(5) of the Act for what must be recorded in relation to alternative measures.

Table 2: Areas in which alternative measures can be taken:

Areas listed in respect of U2U services Sections 10(4) and 12(8) of the Act	**Areas listed in respect of search services** Sections 27(4) and 29(4) of the Act
a) regulatory compliance and risk management arrangements; b) design of functionalities, algorithms and other features; c) policies on terms of use; d) policies on user access to the service or to particular content present on the service; including blocking users from accessing the service or particular content; e) content moderation, including taking down content; f) functionalities allowing users to control the content they encounter, including those functionalities for content encountered especially by children; g) user support measures; and, h) staff policies and practices.	a) regulatory compliance and risk management arrangements; b) design of functionalities, algorithms and other features relating to the search engine; c) functionalities allowing users to control the content they encounter in search results, including those functionalities for content encountered in search results especially by children; d) content prioritisation; e) user support measures; and, f) staff policies and practices.

5.5 A provider should include in its written records the date that its alternative measures came into effect.

When should the written record of alternative measures be made?

5.6 The written record of an alternative measure should be made promptly after the alternative measure has been taken. Where the alternative measure is already in effect prior to the duty coming into force, the written record should be made promptly after the duty has come into effect.

6. Reviewing compliance

What must service providers do?

6.1 A service provider is required to regularly review its compliance with each of the online safety duties set out in Table 3. A provider must also review its compliance as soon as reasonably practicable after making any significant change to any aspect of the design or operation of the service.

Table 3: A service provider must review its compliance with the following online safety duties:

For regulated U2U services	For regulated search services
a) illegal content (section 10) b) children's online safety (section 12) c) user empowerment (section 15) d) content of democratic importance (section 17) e) news publisher content (section 18) f) journalistic content (section 19) g) content reporting (section 20) h) complaints procedures (section 21) i) terms of service (section 71 and section 72) j) disclosure of information about use of service by deceased child users (section 75)	a) illegal content (section 27) b) children's online safety (section 29) c) content reporting (section 31) d) complaints procedures (section 32) e) disclosure of information about use of service by deceased child users (section 75)

6.2 In conducting a review of compliance, the service provider should consider:

a) whether there have been any changes affecting the service which may have an impact on the duties that apply to it (for example, if the service is designated a Category 1 or Category 2A provider);
b) whether the measures it has adopted are sufficient to secure compliance with the relevant online safety duties as they apply to the service provider; and, if not,
c) what further measures it must take to secure compliance.

When should a review be carried out?

6.3 A service provider must review its compliance with the relevant online safety duties at regular intervals. The frequency of such reviews should take into account, in particular: the service being provided; the online safety duties identified in Table 3 that apply to the

service; the findings of the provider's most recent risk assessment; and the outcome of the provider's last compliance review.

6.4 Reviews should be scheduled by providers and occur with a frequency that allows for a continuous cycle of implementation, monitoring, and review.

6.5 As a minimum, we consider that service providers should undertake a compliance review once a year. This aligns with the frequency of the annual and financial reporting cycle for companies (which may entail a review of the compliance and regulatory duties) and the guidance we have issued to providers on the frequency with which risk assessments should be conducted.[22]

6.6 Where the service provider becomes aware of compliance concerns, or implements new measures, it may be appropriate to conduct earlier or more frequent reviews.

6.7 Service providers are also required to carry out a review whenever there is a significant change to the design or operation of their service.

6.8 Service providers should refer to the Risk Assessment Guidance and Risk Profiles regulatory document for detail on when a change is likely to be significant.[23] Table 14 in Part 3, Section 4 of that Guidance sets out principles and considerations to help service providers decide if a proposed change is likely to amount to a significant change. Part 3, Section 4 also provides a list of examples of design and operational changes that are likely to be significant for these purposes. Such examples include the operation of a new recommender system, the addition or removal of a functionality, and changes to a service's content rules or content prioritisation.

[22] See 'Part 1: Duties and carrying out an illegal content risk assessment' in the Risk Assessment Guidance and Risk Profiles, specifically the section titled 'Review and update at least every 12 months'. Service providers required to complete a Children's Access Assessment must re-do these at least every 12 months (see section 36(3) of the Act).

[23] See Part 3, Section 4 of Risk Assessment Guidance and Risk Profiles.