Protecting people from illegal harms online

Annex 6: Guidance on record keeping and review

DRAFT FOR CONSULTATION

Published 9 November 2023
Closing date for responses: 23 February 2024

A6. Guidance on record keeping and review

Introduction

A6.1 Under the Online Safety Act 2023 ('the Act') providers of regulated user to user services and regulated search services are required to keep records of the measures they take to comply with some of their new duties and also to review them regularly. This guidance is intended to assist them to do so.

Who does this guidance apply to?

A6.2 This guidance applies to providers of regulated user-to-user services and/or regulated search services ('service providers').

What does this guidance cover?

A6.3 The guidance covers the duties set out in sections 23 and 34 of the Act on service providers.[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[3] regularly; and

[1] The draft guidance does not cover the record-keeping duties that apply to providers which provide an online service on which pornographic content is published or displayed by or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') or guidance on written records for children's access assessments (conducted under section 36), children's risk assessments (carried out under section 11 or section 28 of the Act). Guidance on these duties will be included in draft guidance for Part 5 providers that we expect to issue in December 2023, and for children's access assessment and children's risk assessments that we expect to issue in March 2024.

[2] A 'Relevant duty' for regulated user-to-user 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 user-to-user 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).

ii) review compliance with the relevant online safety duties as soon as practicable after making a significant change to the design or operation of their service.

A6.4 Our guidance also covers the duty on service providers of Category 1 user-to-user services and Category 2A search services to provide written records of their risk assessments to Ofcom.[4]

A6.5 This guidance should be read alongside the Codes of Practice[5] and our guidance on risk assessments ('Services Risk Assessment Guidance').[6]

Why is this guidance important?

A6.6 This guidance is designed to help service providers understand what is expected of them in relation to keeping written records of measures they take to comply with their relevant duties and reviewing their compliance with the relevant duties.

A6.7 Good, well maintained and clear records and regular, timely reviews of compliance will assist service providers keep track of how they are complying with their relevant duties and ensure that the measures that they have taken are fit for purpose. The records will also provide a useful resource for Ofcom in monitoring how the relevant duties are being fulfilled.

A6.8 The record-keeping and review duties are enforceable by Ofcom. When considering whether a service provider has complied with them, we will take into account whether it has acted in accordance with this guidance.

Guidance on written records

A6.9 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

A6.10 Written records can 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

A6.11 Written records should be legible and written in as simple and clear language as possible. In particular, they should not include jargon, encryption, shorthand or code such that Ofcom cannot understand what they say.

[4] Section 23(10) and section 34(9) respectively of the Act. Category 1 user-to-user 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] The draft illegal harms codes of practice are in Annexes 7 and 8.

[6] The draft Services Risk Assessment Guidance is in Annex 5.

A6.12 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, the records must be capable of being translated into English.

Up-to-date

A6.13 A written record must be kept of a current risk assessment and any measure taken to comply with a relevant duty. While the record must be updated to capture changes made to the measure in question,[7] 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.

A6.14 The written record should be dated when it is made and on each occasion that it is updated.[8]

A6.15 Unless the record in question has been provided to Ofcom, written records which are no longer current should be retained in accordance with the service provider's record retention policies, or a minimum of five years (either calendar or financial), whichever is the longer.

Making and keeping written records of risk assessments

What must service providers do?

All service providers

A6.16 Service providers are required to make and keep a written record of every risk assessment, in easily understandable form, for all aspects of:

a) their illegal content risk assessments;[9] and,
b) their children's risk assessments, if applicable.[10]

A6.17 The record should include details of how the risk assessment was carried out and its findings, including:

a) how a service has consulted Ofcom's risk profiles;
b) the evidence used to assess risks; and,
c) the outcomes of the risk assessment.

A6.18 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, section 11, section 26 or section 28 (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 user-to-user services and/or Category 2A search services - duty to provide risk assessments to Ofcom

A6.19 As soon as reasonably practicable after making or revising a written record of an illegal content or a children's risk assessment, Category 1 user-to-user services and Category 2A

[7] See paragraphs A6.37-A6.43 below 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 below (paragraphs A6.25, A6.30 and A6.36) when the respective written records should be made.
[9] Section 9 and section 26 of the Act.
[10] Section 11 and section 28 of the Act.

search services are required to provide this written record (in full) to Ofcom.[11] 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.

A6.20 We anticipate that services will make records of their risk assessments as they are carrying them out and therefore should be in a position to send them to Ofcom as soon as the risk assessment or revision is concluded.

What should the risk assessment record include?

A6.21 A regulated provider's record of its risk assessment must provide details about how it was carried out and its findings.

A6.22 The record should include the following information:

a) What service the risk assessment applies to;
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;
e) Who had oversight of and/or approved the findings of the risk assessment.

A6.23 The record should also include the following information regarding how a service has undertaken the risk assessment, and its findings:

a) Confirmation that a service has consulted Ofcom's Risk Profiles. A service may do this by recording the outcomes of the Risk Profiles questionnaire, provided in Appendix A of the Services Risk Assessment Guidance;
b) A record of any risk factors from Ofcom's Risk Profiles which are relevant to the regulated provider's service;
c) Where applicable, a list of any additional characteristics (including user base, business models, functionalities, governance and systems and processes) the regulated provider have considered alongside the risk factors identified in Ofcom's Risk Profiles;
d) A list of the evidence that has informed the assessment of likelihood and impact of each kind of priority illegal harm;
e) The level of risk assigned to each of the 15 kinds of illegal harm and any relevant non-priority illegal harm, and an explanation of the decision. Where appropriate, this should also include the level of risk assigned to sub-categories of harm (including CSAM and Grooming);
f) Confirmation that the findings of the risk assessment have been reported through appropriate governance channels;
g) Information regarding how a service takes appropriate steps to keep the risk assessment up to date (for example, a written policy).

A6.24 Providers should refer to the relevant Services Risk Assessment Guidance for more detailed guidance on how to carry out a risk assessment.

When should the risk assessment record be made?

A6.25 We anticipate that the written record of the risk assessment (or a revision to the risk assessment) will be made contemporaneously to ensure it is accurate and up-to-date.

[11] Section 23(10) and section 34(9) of the Act respectively.

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

What must service providers do?

A6.26 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 below in Table A6.1, they should keep a written record of it.

Table A6.1: relevant duties for service providers

'Relevant duties' for providers of regulated user-to-user services	'Relevant duties' for providers of regulated search services
Illegal content (section 10)	Illegal content (section 27)
Children's online safety (section 12)	Children's online safety (section 29)
User empowerment (section 15)	Content reporting (section 31)
Content of democratic importance (section 17)	Complaints procedures (section 32)
Journalistic content (section 19)	
Content reporting (section 20)	
Complaints procedures (section 21)	

What should the record include?

A6.27 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 on which the measure takes effect.

A6.28 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.

A6.29 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 of that document or information) should be kept and maintained as part of the record for the purposes of the duty under section 23(3) or section 34(3).

When should the record of a Code measure be made?

A6.30 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, then the written record should be made promptly after the duty has come into effect.

Records of alternative measures taken to comply with a relevant duty

What must service providers do?

A6.31 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, service providers do not need to follow a Code of Practice if they take, or already have, alternative measures to comply with a relevant duty.

A6.32 If a service provider adopts, or has already adopted, alternative measures to those set out in the Code of Practice to comply with their relevant duties (see Table A6.1) then they must make and keep a written record of the alternative measures.

What should the record of an alternative measure include?

A6.33 Written records must include:

a) the applicable measures[12] in a Code of Practice that have not been taken or are not in use;[13]
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).

A6.34 Where service providers adopt alternative measures to comply with the safety duties in relation to illegal content[14] or the safety duties protecting children,[15] the written record must also state whether the alternative measures have been taken or are in use in every area listed in Table A6.2 (to the extent there are applicable measures in a Code of Practice):[16]

Table A6.2: areas in which alternative measures must be taken or be in use

Areas listed in respect of regulated user-to-user services[17]	Areas listed in respect of search services[18]
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	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

[12] These are measures set out by Ofcom in a Code of Practice which apply to the relevant service provider.
[13] There is no obligation on service providers to keep a written record of a measure (from the Code of Practice) that does not apply to them (for example, where particular measures only apply to a subset of services based on size or risk of a particular harm).
[14] Specifically, the duties in section 10(2) and (3) for user-to-user services and section 27(2) and (3) for search services.
[15] Specifically, the duties in section 12(2) and (3) for user-to-user services and section 29(2) and (3) for search services.
[16] See section 23(5) and section 34(5) of the Act.
[17] See section 10(4) and section 12(8) of the Act.
[18] See section 27(4) and section 29(4) of the Act.

Areas listed in respect of regulated user-to-user services[17]	Areas listed in respect of search services[18]
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.	functionalities for content encountered in search results especially by children; d) content prioritisation; e) user support measures; and, f) staff policies and practices.

A6.35 Providers should include in their written records the date their alternative measures came into effect.

When should the written record of alternative measures be made?

A6.36 The written record of alternative measures 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, then the written record should be made promptly after the duty has come into effect.

Reviewing compliance

What must service providers do?

A6.37 Service providers are required to regularly review their compliance with each of the online safety duties set in Table A6.3. They must also review their compliance as soon as practicably possible after making any significant change to any aspect of the design or operation of the service.

Table A6.3: Service providers must review their compliance with the following online safety duties

For regulated user-to-user services	For regulated search services
Illegal content (section 10)	Illegal content (section 27)
Children's online safety (section 12)	Children's online safety (section 29)
User empowerment (section 15)	Content reporting (section 31)
Content of democratic importance (section 17)	Complaints procedures (section 32)

For regulated user-to-user services	For regulated search services
News publisher content (section 18) Journalistic content (section 19) Content reporting (section 20) Complaints procedures (section 21) Terms of service (section 71 and section 72) Disclosure of information about use of service by deceased child users (section 75)	Disclosure of information about use of service by deceased child users (section 75)

A6.38 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?

A6.39 Service providers must review their compliance with the relevant online safety duties at regular intervals. The frequency of such reviews should take into account, in particular: the service they provide; the online safety duties identified in Table A6.3 that apply to them; the findings of their most recent risk assessment; and, the outcome of their last compliance review.

A6.40 Reviews should be scheduled by providers and occur with a frequency that allows for a continuous cycle of implementation, monitoring and review.

A6.41 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 their compliance and regulatory duties) and the guidance we have issued to providers on the frequency of which they should undertake their risk assessments.[19]

A6.42 Where the service provider becomes aware of compliance concerns, or implements new measures, it may be appropriate to conduct earlier or more frequent reviews.

A6.43 Service providers are also required to carry out a review whenever there is a significant change to the design or operation of their service. Service providers should refer to the Services Risk Assessment Guidance on when a change is likely to be significant and the examples of design and operational changes which are likely to be significant.[20] The latter

[19] See Annex 5 (Services Risk Assessment Guidance), table 5.2, page 18. Service providers required to complete a Children's Access Assessment must redo these at least every 12 months (see section 36(3) of the Act).
[20] See Annex 5 (Services Risk Assessment Guidance), paragraphs A5.53 – A5.56.

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.