Statement: Technology Notices Guidance

Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023

Statement

Published 8 May 2026

Contents

Section

1. Overview 3
2. Introduction 5
3. How we approach our decision to issue a Technology Notice 10
4. Initial assessment 41
5. Next steps and approach to information gathering 46
6. Deciding whether to issue a Technology Notice 55
7. Next steps after issuing a Technology Notice 62
8. Disclosure of information and publication 68

Annexes

A1. Regulatory framework 73
A2. Impact Assessments 86
A3. Glossary 91

1. Overview

1.1 Ofcom is the United Kingdom's (UK) communications regulator, overseeing sectors including telecommunications, post, broadcast TV, radio, and online services. We were appointed the online safety regulator under the Online Safety Act 2023 (the Act) in October 2023.

1.2 Part 7 of the Act sets out Ofcom's powers and duties in relation to regulated services. These include specific powers under Chapter 5 of Part 7 of the Act for Ofcom to issue notices to regulated services to deal with two specific types of illegal content: terrorism and/or child sexual exploitation and abuse (CSEA) content. We refer to such a notice as either a 'Technology Notice' or a 'Notice' throughout this document.

1.3 Under the Act, Ofcom is required to produce and publish guidance for providers of regulated user-to-user and regulated search services about how we propose to exercise our Technology Notice functions.

1.4 We published a consultation document and draft guidance in December 2024 (the December 2024 Consultation). In this statement, we set out our assessment of the feedback we received from respondents to our consultation alongside our Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023 (the Guidance).

What we have decided – in brief

We have broadly confirmed our proposed guidance as set out in the December 2024 Consultation about how we propose to exercise our Technology Notice functions.

However, having considered respondents' comments on our draft guidance we have made some changes to provide further clarity. In particular, in the Guidance we clarify:

- when Ofcom will engage with service providers during each stage of the Technology Notice process and when there will be opportunities for service providers to make representations to Ofcom;
- the assistance that should be provided to the skilled person by the service provider and related parties;
- that a service provider will be provided with a copy of the skilled person's report (in final form) alongside a Warning Notice;
- when considering whether it is necessary and proportionate to issue a Technology Notice, Ofcom will consider in all cases the technical feasibility for the service provider of doing what would be required of them in the Technology Notice;
- the financial costs associated with accredited technology that Ofcom will consider when considering whether it is necessary and proportionate to issue a Technology Notice;
- that Ofcom will not require the service provider to make any technology it has developed pursuant to a Technology Notice available for use by other service providers; and
- the process that Ofcom will follow where we are intending to issue a Notice to require the use of a developed/sourced technology.

We have also made some minor amendments to a number of paragraphs in the guidance in order to clarify our drafting.

2. Introduction

2.1 This statement is about the Guidance we have produced to support the use of Ofcom's new powers in Chapter 5 of Part 7 of the Act. Under section 127 of the Act, Ofcom is required to produce guidance for providers of regulated user-to-user and regulated search services (Part 3 services) on how we propose to exercise our Technology Notice functions.[1]

2.2 This introduction covers:

a) Ofcom's powers in relation to Technology Notices. Annex 1 contains further details on the regulatory framework;

b) a short summary of the December 2024 Consultation and stakeholder responses. A more detailed summary of stakeholder responses, and our position on these points, is set out in sections 3-8 of this Statement; and

c) the next steps that must be taken before Ofcom can issue a Technology Notice.

Background

2.3 Under the Act, providers of Part 3 services have a range of new duties, including in relation to illegal content. They must assess the risk of harm arising from illegal content or activity on their regulated services and take or use proportionate measures to effectively manage and mitigate those risks. They must also take or use proportionate measures to prevent individuals from encountering 'priority' illegal content by means of their regulated services.

2.4 Ofcom has published the Illegal Harms Codes of Practice which set out recommended measures that service providers can take to comply with their illegal content safety duties. Ofcom can take enforcement action where providers breach their illegal content safety duties, which may include where they do not take recommended measures or appropriate alternative measures to comply. Ofcom has also published the Online Safety Enforcement Guidance which explains when and how Ofcom will consider taking enforcement action.

2.5 In addition to these duties for service providers, the Act gives Ofcom additional powers to tackle terrorism and CSEA content on regulated Part 3 services. Under section 121 of the Act, Ofcom has the power to issue a Technology Notice to the provider of a Part 3 service where we consider it necessary and proportionate to deal with terrorism or CSEA content (or both). Sections 122-126 of the Act contain further provisions setting out the processes and procedures that Ofcom must follow in the event that it exercises this power.

Terrorism and CSEA content

The most serious categories of illegal content covered by the Act include terrorism and CSEA content, and all providers need to act to prevent users encountering such content.

Terrorism content refers to content which amounts to an offence specified in Schedule 5 to the Act. These offences include, for example, offences relating to 'proscribed organisations',

[1] See section 127 of the Act. Regulated user-to-user and regulated search services are defined in the Act as 'Part 3 Services' because Part 3 of the Act imposes duties on providers of these services. We have adopted this definition throughout this statement.

information likely to be of use to a terrorist and encouraging terrorism or disseminating terrorist materials.

CSEA content refers to content which amounts to an offence specified in Schedule 6 to the Act. These offences include, for example, offences relating to the making, showing, distribution or possession of an indecent image or film of a child, linking to or directing a user to child sexual abuse material (CSAM) and possession of a paedophile manual.

Annex 1 explains in more detail what terrorism and CSEA content are.

2.6 A Technology Notice could require a Part 3 service provider to:

a) use technology that has been accredited (accredited technology), by Ofcom or another person appointed by Ofcom, to identify and/or prevent individuals from encountering terrorism content communicated publicly; [2] and/or

b) use accredited technology to identify and/or prevent individuals from encountering CSEA content communicated publicly or privately. A provider could alternatively be required to use best endeavours to develop or source technology that meets minimum standards of accuracy to deal with such CSEA content.[3]

2.7 Ofcom's power to require the use of a technology through Technology Notices differs in some important ways from our power to recommend measures in a Code of Practice. For example:

a) Technology Notices are focused on the use, development, or sourcing of technology to deal with terrorism/CSEA content only, unlike Code measures which can relate to the wider design or operation of the service and a broader range of illegal/harmful content;

b) Codes of Practice set out recommended measures which, if adopted in full, would result in the provider of a regulated service to which those measures apply being treated as complying with its safety duties. However, providers can adopt alternative measures to comply with their duties and, if they do so, are required to comply with additional record-keeping duties (which include keeping a record of how those alternative measures amount to compliance with the duty in question);

c) By contrast, a Technology Notice would impose an enforceable legal requirement that the provider of a regulated service deploy specific accredited technology to deal with terrorism/CSEA content on that service. For the purposes of dealing with CSEA, a Technology Notice could also require that a service use best endeavours to develop or source relevant technology; and

d) Ofcom cannot recommend in Codes of Practice the use of proactive technology to analyse content communicated 'privately', or meta

[2] The minimum standards of accuracy are minimum standards of accuracy for the detection of terrorism and/or CSEA content (as the case may be).

[3] The wording of the Act distinguishes between how Technology Notices may apply to regulated user-to-user services and regulated search services. For regulated user-to-user services, a Notice may require a provider to use accredited technology to identify and swiftly take down or prevent individuals from encountering terrorism and/or CSEA content. For regulated search services, a Notice may require a provider to: use accredited technology to identify search content of its service that is terrorism and/or CSEA content; and to swiftly take measures designed to secure that, as far as possible, search content of the service no longer includes terrorism and/or CSEA content identified by the technology. See section 121(2) and (3) for more information on the provisions for regulated user-to-user and regulated search services respectively.

e) data relating to that content. Section 121 is the only provision in the Act which gives Ofcom the power to require the use of proactive technology to analyse content communicated privately (and this power only applies in respect of CSEA Technology Notices).

2.8 A more detailed summary of the regulatory framework relevant to Technology Notices is set out in Annex 1. In particular, the Annex explains in more detail:

a) Ofcom's powers under the Act to tackle illegal harms and specifically terrorism and CSEA content;

b) our powers under section 121 of the Act, including their position within the wider regulatory regime and the steps required and other considerations for Ofcom before we can issue a Technology Notice; and

c) Ofcom's general duties relevant to the exercise of our Technology Notice functions.

Our draft guidance

2.9 As explained above, section 127 of the Act requires Ofcom to produce and publish guidance for the providers of Part 3 services about how we propose to exercise our Technology Notice functions. We must have regard to this guidance when exercising, or deciding whether to exercise, those functions, and keep the guidance under review.

2.10 In December 2024, we consulted on draft guidance for the providers of Part 3 services. The draft guidance explained how we proposed to exercise our Technology Notice functions, setting out in particular what a Notice might require Part 3 service providers to do, the process we would typically follow when deciding whether it is necessary and proportionate to issue such a Notice and detail on the matters to which we would expect to have regard when making our decision.

2.11 The draft guidance stated that it was intended to provide procedural guidance regarding the steps Ofcom would expect to take, and the matters we would expect to consider, when exercising (and deciding whether to exercise) our Technology Notice functions. It also set out that any decision as to whether a Technology Notice is necessary and proportionate in a particular case would be highly fact-specific and taken in the round, taking into account the matters we must consider under the Act and any other matters or considerations that might be relevant to our assessment. As such, we explained in our December 2024 Consultation that the draft guidance did not seek to set out in detail the circumstances when we might consider it necessary and proportionate to issue a Technology Notice.

Structure of this statement

2.12 We received 810 responses to our consultation. Of these, 782 related to a civil society campaign organised by Open Rights Group in support of end-to-end encryption (E2EE). A memorandum summarising the key themes of these submissions, along with copies of the additional 22 non-confidential responses received, can be found on our website.[4] We are grateful to all respondents for their submissions. In this statement we summarise those consultation responses relating to our Guidance and set out our assessment of that feedback in explaining our finalised Guidance.

[4] Consultation: Technology Notices - Ofcom

2.13 We note that our December 2024 Consultation also consulted on our policy proposals for minimum standards of accuracy in the detection of terrorism and CSEA content. These are standards against which technology needs to be accredited before it can be required in a Technology Notice, and in relation to which Ofcom must provide advice to the Secretary of State. Unless stated otherwise, we do not consider in this statement any stakeholder feedback that related specifically to those proposals, which are addressed in our document 'Research, evidence and advice to the DSIT Secretary of State on how to set minimum standards of accuracy'.

2.14 The remainder of this statement adopts the same structure as the draft guidance. In each section, we summarise what we said in the corresponding section of the draft guidance. We then outline stakeholder feedback received in response to the December 2024 Consultation on principal themes within that section and explain the decisions we have taken in response in developing our Guidance.

2.15 We have not included separate sections addressing sections A1 (Overview) and A2 (Introduction) of the draft guidance. This is because we did not receive any specific comments from stakeholders on section A1. We did receive some comments that were relevant to section A2, regarding data protection and complaints procedures, but as these comments also relate to section A3 (How we approach our decision to issue a Technology Notice) of the draft guidance we have included our response in each case in section 3 of this statement.

2.16 We note, however, that we have also amended section 2 of the Guidance to refer to Ofcom's duties to have regard to:

a) the desirability of encouraging investment and innovation in relevant markets (see paragraph 2.34);

b) the desirability of promoting economic growth in exercising our regulatory functions, referred to as 'the Growth Duty' (see paragraph 2.35);

c) the Statement of Strategic Priorities that has been designated by the Secretary of State for Online Safety (see paragraph 2.36); and

d) the Equality Act 2010 (see paragraphs 2.39 to 2.41).

What happens next

2.17 Ofcom has also today published its advice to the Secretary of State on how to set minimum standards of accuracy. It is important to highlight that just because a technology is accredited as meeting minimum standards of accuracy set out by the Secretary of State does not necessarily mean that Ofcom will require its use by a particular regulated service. The accreditation process is only intended to determine whether a technology could be considered for requirement through a Notice. For the avoidance of doubt, this statement, and the accompanying guidance, do not set out the accreditation process.

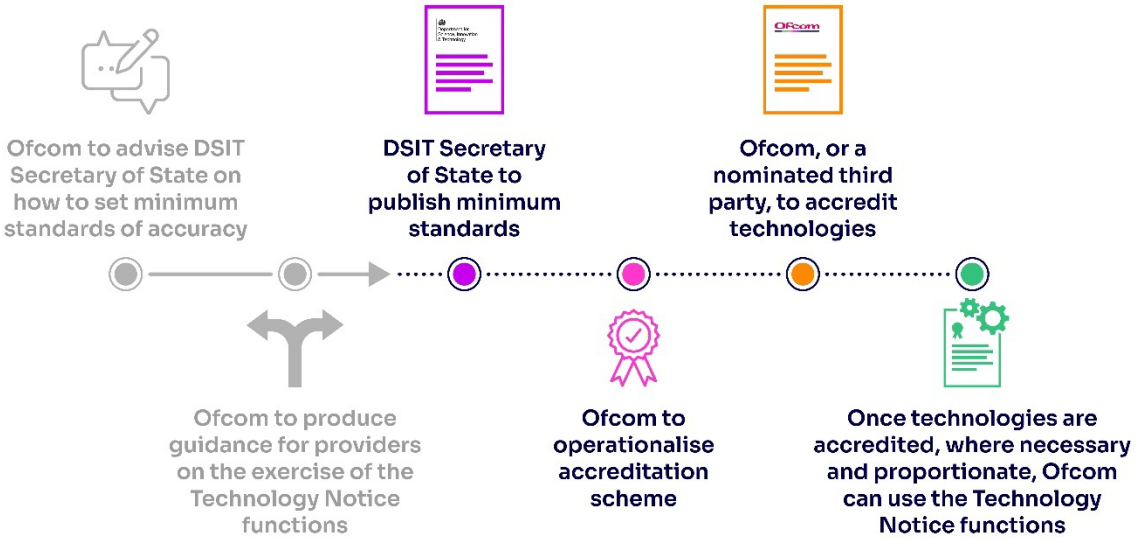
2.18 It is important to note that, in addition to publishing our Guidance, there are certain other steps that must have been taken before Ofcom can consider issuing a Technology Notice:

a) Following receipt of Ofcom's advice, it is then for the Secretary of State to approve and publish minimum standards of accuracy;

b) Once the Secretary of State has approved and published minimum standards of accuracy, Ofcom is then responsible for setting up a process to accredit technologies as meeting those minimum standards; and
c) Ofcom or a nominated third party must accredit technology against the minimum standards of accuracy.

2.19 Our roadmap to regulation sets out our latest plans for implementation of the online safety regime.

Figure 1 – Steps required to operationalise the Technology Notice functions



3. How we approach our decision to issue a Technology Notice

Introduction

3.1 Section 3 of the Guidance explains how we will approach our assessment of whether it is necessary and proportionate to issue a Technology Notice. It covers:

a) The matters we must consider when deciding if a Technology Notice is necessary and proportionate (the Specified Matters);

b) Other matters we are likely to consider; and

c) How we will approach our assessment of whether it is necessary and proportionate to issue a Technology Notice, including the appropriateness of compatibility testing.

3.2 We received feedback on this section from a range of stakeholders, including service providers, civil society organisations, child safety organisations, the Information Commissioner's Office (the ICO), technology developers and academic researchers.

3.3 Child safety organisations generally supported robust use of Technology Notice powers,[5] and welcomed the recognition in the draft guidance that Ofcom expected to consider victims' rights including, in the case of CSEA content, the right to privacy of victims of child sexual abuse and to the protection of their personal data.[6] The ICO welcomed Ofcom's high-level observations on our approach to the Specified Matters, consideration of safeguards to mitigate risks arising from false positives, and our proposal to consider compatibility testing which they described as "a valuable safeguard" against the occurrence of inaccurate decisions where solely automated decision-making is used.[7]

3.4 The responses we received did not request extensive changes to the guidance but there were concerns raised about how Ofcom would use the Technology Notices powers in specific circumstances and some stakeholders requested further clarity in the guidance.[8] In particular, some queried how Ofcom would balance competing rights and interests and ensure appropriate safeguards.[9]

3.5 Having carefully considered the comments provided in response to our consultation, and for the reasons set out in this section, we are satisfied that section 3 of the Guidance should be broadly in line with our draft guidance. However, we have made a small number of amendments, including in light of stakeholder comments, which we discuss below.

---

[5] IWF response to Ofcom's December 2024 Consultation, p.7; NSPCC response to Ofcom's December 2024 Consultation, pp.5-6; Marie Collins Foundation response to Ofcom's December 2024 Consultation, p.6.
[6] IWF response to Ofcom's December 2024 Consultation, p.2 and p.10.
[7] ICO response to Ofcom's December 2024 Consultation, pp.10-11.
[8] Google response to December 2024 Consultation, pp.13-15; [✂] response to December 2024 Consultation, p.4 and p.6; [✂] response to December 2024 Consultation, pp.15-17; X response to December 2024 Consultation, p.5; Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.6.
[9] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.8; Marie Collins Foundation response to December 2024 Consultation, p.6; IWF response to December 2024 Consultation, p.7.

Overview of stakeholder responses

3.6 We received responses asking for amendments to section 3 of the Guidance on the following key themes:

a) Specified Matters;

b) Other matters Ofcom expect to consider;

c) Threshold for intervention;

d) Fundamental rights impacts;

e) Technology Notices to develop or source technology;

f) Compatibility testing; and

g) Specific requirements of a Technology Notice.

Specified Matters

Summary of draft guidance

3.7 Paragraphs A3.5 to A3.7 of our draft guidance set out each of the matters that we are required to consider when deciding whether it is necessary and proportionate to issue a Technology Notice, and referred to these as 'Specified Matters'.[10] The draft guidance then provided some high-level observations on the Specified Matters, including that the Act does not provide that any of the Specified Matters carries any greater weight than another.

Summary of stakeholder responses

3.8 Some stakeholders suggested the draft guidance was unclear about how Ofcom will consider some of the Specified Matters. In particular:

a) Two stakeholders encouraged Ofcom to provide further guidance on how we will consider the "prevalence of relevant content on the service, and the extent of its dissemination" by means of the service.[11] Google in particular suggested that Ofcom should define 'prevalence' in this context and should clarify how we will determine prevalence and the extent of dissemination of such content (including what metrics will be used) to assess whether a Technology Notice is necessary and proportionate. They also stated we should clarify that we will work with the service provider in question, as part of our initial assessment, to determine the most appropriate metrics;[12] and

b) The ICO commented that the draft guidance does not specify how Ofcom will take the "level of risk or the likelihood of a data breach" into account when deciding whether a Technology Notice is necessary and proportionate.[13]

3.9 The NSPCC suggested the rights of victims of CSAM should be central when weighing up the privacy implications of issuing a Technology Notice. They stressed the importance of

[10] The "Specified Matters" that Ofcom must consider particularly consider are set out in section 124(2) of the Act and are included in paragraph 3.5 of the Guidance.
[11] Google response to December 2024 Consultation, pp.13-14; [✂] response to December 2024 Consultation, p.6.
[12] Google response to December 2024 Consultation, pp.14-15.
[13] ICO response to December 2024 Consultation, p.9.

limiting the number of people who encounter CSAM, noting that it is a severe violation of victims' rights to have such content reshared and viewed by others.[14]

3.10 Another stakeholder also invited Ofcom to provide more detailed guidance on our assessment of some of the Specified Matters, particularly clarification that we would consider (and discuss with providers):

a) a provider's existing deployment of technologies or safety by design features when considering the "systems and processes used by the service which are designed to identify and remove relevant content"; and

b) their ability to adopt their own existing or adapted technology as a "less intrusive measure" than the imposition of a Technology Notice.[15]

3.11 Similarly, X requested more clarity on how Ofcom will consider the effectiveness of providers' existing safety measures.[16]

3.12 One stakeholder suggested that Ofcom should assess whether accredited solutions are applicable and compatible with a service's existing moderation framework and, where possible, service providers should be allowed to enhance their current systems rather than be required to adopt entirely new technologies.[17]

3.13 Another stakeholder considered that service providers are best placed to assess whether terrorism or CSEA content detection technologies are proportionate because they can more accurately consider the facts and circumstances of their service and typical use, including whether a less intrusive measure is available and appropriate.[18]

3.14 A different stakeholder said it was unclear, at paragraph A3.7(d) of the draft guidance, why privately communicated content could ever be relevant to Ofcom's judgement on issuing a Technology Notice for publicly communicated terrorism content because Ofcom's power to issue a Notice is limited to content communicated publicly, and that Ofcom should use evidence related to public content and evidence of harm in public content alone.[19]

3.15 Some stakeholders commented on the weight that should apply to the Specified Matters:

a) Drs Shurson, Keenan and Ó Floinn stated that the draft guidance provided no indication as to how the relevant factors would be weighed, and suggested that considerations regarding privacy, data protection, freedom of expression and journalistic content, alongside the availability of less intrusive measures, must be prioritised in making a proportionality assessment;[20]

b) While agreeing that the Act did not require Ofcom to place greater weight on any of the Specified Matters, one stakeholder considered that Ofcom should prioritise actual evidence of harm, such as "the prevalence of relevant content on the service, and the extent of its dissemination" over other Specified Matters that reflect theoretical risk,

[14] NSPCC response to December 2024 Consultation, pp.5-6.
[15] [✂] response to December 2024 Consultation, pp.15-16.
[16] X response to December 2024 Consultation, p.5.
[17] [✂] response to December 2024 Consultation, p.2. [✂]
[18] [✂] response to December 2024 Consultation, p.4.
[19] [✂] response to December 2024 Consultation, p.4.
[20] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.8.

such as "the kind of service it is" and "the functionalities of the service", to target the risk to users that actually materialises; [21] and

c) As discussed in more detail at paragraph 3.47(b) below, some stakeholders suggested that safety (i.e., the risk to users) should take precedence over considerations of financial cost.

3.16 Two stakeholders asked Ofcom to consider providing specific/practical examples as to how we will weigh the Specified Matters. [22]

Our response

3.17 Having carefully considered stakeholders' submissions, and for the reasons set out below, we are satisfied that the guidance on which we consulted remains appropriate and that no amendments are warranted.

3.18 However, we recognise the desire from stakeholders for greater clarity and note that we are required to keep the Guidance under review (and will update it where we consider it appropriate to do so based on our experience in administering the online safety regime).

Requests for greater clarity on certain Specified Matters

3.19 We note the calls from stakeholders for Ofcom to define "prevalence" in the Guidance and to clarify how we will determine "prevalence and the extent of dissemination" of relevant content (including what metrics will be used) to assess whether a Technology Notice is necessary and proportionate. However, we are not persuaded that it is necessary or appropriate for us to provide further detail on this in the Guidance:

a) this approach is consistent with our approach in other regulatory documents, where we have not sought to rigidly define either of these concepts. [23] We note though that, as the concepts of 'prevalence' and 'dissemination' are not defined in the Act, we would expect in the first instance to consider their ordinary dictionary meaning; and

b) any decision on which metrics are appropriate when considering prevalence and dissemination of terrorism and CSEA content will need to be made on a case-by-case basis according to the features of the relevant service. We do not therefore consider it would be appropriate to set out a prescriptive list in the Guidance about the types of metrics we would consider and inappropriately fetter our discretion in this regard. While not an exhaustive list, we note however that this may include consideration of the proportion of all such content on a service including, where relevant, the extent to which such content is disseminated by a recommender system or search engine; evidence that the prevalence of content has persisted over time; how often the content is recommended to users; and the degree of user engagement/interaction with the content including the proportion of all items a user interacts with that are terrorism and/or CSEA content. As noted in paragraph 5.10 of the Guidance, we may also gather information from other sources such as law enforcement agencies and public sources

[21] [✂] response to December 2024 Consultation, p.4.
[22] [✂] response to December 2024 Consultation, p.15; X response to December 2024 Consultation, p.2 and p.5.
[23] Ofcom has published a document entitled "Evaluating Online Safety Measures" in May 2024. This does not seek to define the term "prevalence" but does acknowledge in paragraph 2.53 some of the difficulties in measuring prevalence and that the ways in which services identify and capture details of the amount of harmful content may vary.

(including users of the service and offenders), which may be particularly relevant when considering the prevalence of privately communicated content.

3.20 We can confirm that a provider's existing deployment of technologies will be considered as part of the Specified Matters. In particular, this would be taken into account when considering the systems and processes used by the service which are designed to identify and remove relevant content (as required by section 125(2)(g) of the Act) and whether the use of any less intrusive measures would be likely to achieve a significant reduction in the amount of relevant content (as required by section 125(2)(l)). We do not consider that the Guidance needs to be amended in this regard. When considering whether a Notice requiring the use of accredited technology may be more appropriate than a Notice to develop or source technology, we would also typically expect to consider a provider's existing deployment of technologies (or technologies that it might be in the process of developing).[24] We note however that, where terrorism and/or CSEA content are prevalent on a service despite that service already taking steps (including the deployment of technology) to tackle them, it suggests those steps are not by themselves sufficient.

3.21 As noted in paragraph 4.9 of the Guidance, we may engage with the service provider during the initial assessment stage (and will engage with them in any event before issuing a Warning Notice) to request the provision of information to assist us in considering the Specified Matters, including the prevalence of content and its dissemination and the measures that they already have in place to deal with terrorism/CSEA content (as appropriate). As part of this engagement, we would expect the service provider in question to be able to give their views on the appropriateness of specific metrics. As discussed in section 5, these are also matters that we may ask the skilled person to report on (and, if we do, we will provide a copy of the skilled person's report (in final form) and the provider in question will have the opportunity to provide representations on it).

3.22 We have considered the ICO's comment that the draft guidance did not specify how we will take account of the level of risk or the likelihood of a data breach when deciding whether a Technology Notice is necessary and proportionate in a particular case. We are not however persuaded that it is necessary for our Guidance to provide further detail on this at this stage. As noted at paragraph 3.106(c) below, where we are considering issuing a Technology Notice, we would expect this to trigger discussion between the ICO and Ofcom about how our teams may be able to collaborate and about the extent to which we may be able to share information. We would expect us to consider how our teams may be able to collaborate on considering the level of risk or likelihood of a data breach.

3.23 As regards terrorism content, our power to issue a Technology Notice is limited to content communicated publicly. However, as noted in paragraph 3.7(d) of the Guidance there may be circumstances where we have evidence that terrorism content is prevalent or disseminated on private communications. While we recognise the need to exercise caution when taking account of this in any decision on whether to issue a Technology Notice regarding terrorism content, and our focus in such a case should be on terrorism content

[24] Consistent with this, we note that (as discussed at paragraph 3.132 below), we have made some modifications to our guidance regarding compatibility testing. These include amendments to make clear that such testing may be appropriate to: (a) ascertain how accredited technology might be deployed alongside the providers' existing systems and processes; and/or (b) where the provider in question already deploys technology to detect terrorism or CSEA content (or is in the process of developing such technology) to assess the performance of that technology against specific metrics, and with a view to identifying whether it may be more proportionate to issue a Notice to develop or source technology in that case.

communicated publicly, our view also remains that where we have evidence that terrorism content is prevalent or disseminated on private communications that may also be indicative of the presence of terrorism content communicated publicly. We are concerned that it would not be appropriate for the Guidance to preclude us from taking account of such relevant evidence in a particular case. We have amended paragraph 3.7(d) of the Guidance to make this clearer.

Weight given to each of the Specified Matters

3.24 While a number of stakeholders suggested that Ofcom should attach greater weight to some of the Specified Matters over others, we have not amended the draft guidance to suggest that any particular matters should be prioritised over others. We will instead weigh all relevant considerations in the round when reaching our decision about necessity and proportionality in a particular case.

3.25 We note in this regard that the Act does not require us to place greater weight on any particular Specified Matters when deciding whether it is necessary and proportionate to issue a Technology Notice in a particular case. Nor does it provide that those matters should be given greater weight than any other matters that Ofcom considers relevant.

3.26 We recognise the points raised by some stakeholders about the importance of some of the Specified Matters (and of the other matters that we said we would consider, and which are discussed from paragraph 3.30 below). These include the importance of considering the impacts of a Technology Notice on individuals' rights (including as to privacy and freedom of expression), the importance of reducing terrorism/CSEA content, and the importance of considering evidence of actual harm. Specifically in relation to CSEA content, the right to privacy of victims of child sexual abuse was noted in paragraph 3.9 (c) of the Guidance. However, we disagree that the Guidance should state we will place greater weight on these matters than others (such as the kind of service, and functionalities of the service). It is not clear to us that such an approach would be consistent with the statutory framework, and we are satisfied that the Guidance as drafted will enable us to reach a sound decision on whether it is necessary and proportionate in a particular case.

3.27 In relation to the impact of a Technology Notice on individuals' rights, and as noted in paragraph 2.37 of the Guidance, we also note that Ofcom is required by section 6 of the Human Rights Act 1998 to act in a way which is compatible with the ECHR. We recognise that the use of terrorism and/or CSEA content detection technologies in practice could have significant impacts on users' rights (including to freedom of expression and to privacy), as well as the rights of others. Any interference with fundamental rights needs to be justified. Ofcom has considerable experience in considering such matters, in both its online safety work but also in the other areas that it regulates (including in its regulation of broadcasting).

Practical examples of how we will balance the Specified Matters

3.28 While we recognise desire for practical examples about how we will balance the various matters in specific circumstances, we do not consider that it is necessary or appropriate for the Guidance to include such examples at this stage. As stated in paragraph 3.4 of the Guidance, any decision about whether to issue a Technology Notice will be highly fact-specific and we are not therefore persuaded that such examples would be helpful for readers. Where we consider that there could be value in including examples based on our experience of administering the Technology Notice regime in due course however, we may update the Guidance.

3.29 For completeness, we note that we do not agree with the suggestion from one stakeholder that service providers are necessarily best placed to assess whether terrorism or CSEA content detection technologies are proportionate (including whether a less intrusive measure may be available and appropriate). While we recognise the value of providers' representations on this, including in response to a Warning Notice, it is ultimately for Ofcom to determine whether it is necessary and proportionate to issue a Technology Notice in a particular case.

Other matters Ofcom expect to consider

Summary of draft guidance

3.30 Paragraph A3.8 of the draft guidance set out other matters that we are likely to consider before issuing a Technology Notice. These were the technical feasibility for the service provider of doing what would be required of them, taking into account the way service is configured; the size and capacity of the provider; the likely financial cost of complying; other rights protected by the ECHR; and the potential impact of the Technology Notice in reducing the amount of terrorism or CSEA content.

Applicability of the other matters

Summary of stakeholder responses

3.31 Drs Shurson, Keenan and Ó Floinn commented that the other matters Ofcom are "likely to consider" are "essential" for each Technology Notice.[25]

Our response

3.32 We have amended paragraph 3.9 of the Guidance to clarify that we expect the other matters listed in subsections (a) to (d)[26] to also be relevant to our consideration of whether it is necessary and proportionate to issue a Technology Notice in each case. However, the Guidance on technical feasibility has been moved to a separate paragraph (see below for further details).

Technical Feasibility

Summary of stakeholder responses

3.33 Some stakeholders requested that Ofcom provide further detail on what is meant by technical feasibility and how it will be determined, noting that 'technical feasibility' is not defined in the Act.[27]

3.34 Some expressed concern about the technical feasibility of requiring the use of accredited technology on E2EE services. For example:

a) as noted in paragraph 3.81(b)(i) below, multiple stakeholders suggested that Ofcom should be clear in the guidance that, if a service is configured with E2EE, a Technology

[25] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.4.
[26] Subsections (a) to (d) relate to: the size and capacity of the provider; the likely financial cost to the service provider of complying with the Notice; any impact on other rights; and the potential impact of the Technology Notice in reducing the amount of terrorism or CSEA content.
[27] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.5.

Notice will not require such encryption to be removed or weakened,[28] or that service providers will be required to scan encrypted content.[29] The Internet Society also asserted that it is technically infeasible to implement `client-side scanning' technology due to issues of inherent systemic risk and the violation of user trust;[30] and

b) the Internet Society suggested that there is a significant conflict in Ofcom's approach to technical feasibility across its Codes of Practice and in its draft Technology Notice guidance.[31] Similarly, [✂] noted the changes made to Ofcom's Illegal content Codes of Practice for user-to-user services (as compared to the version Ofcom consulted on) on the technical feasibility of measures on E2EE services and suggested a similar acknowledgement of technical limitations should be addressed in the guidance.[32]

3.35 The same stakeholder welcomed Ofcom's recognition that it would generally expect to consider technical feasibility even though it is not required to do so under the Act but sought further assurance as to when technical feasibility would be a relevant consideration for Ofcom. It noted that the Secretary of State is always required, under the Investigatory Powers Act 2016 (IPA 2016), to take into account the technical feasibility of compliance with a Technical Capability Notice.[33]

3.36 That stakeholder also stated Ofcom should clarify when a provider might be required to make a change to the design or operation of a service and what would be considered proportionate, noting that any such change would likely entail a significant burden for providers that may not be able to be confined to the UK or UK users.[34] As we discuss further in paragraphs 3.99-3.100 below, the ICO likewise sought clarity in the guidance on what kinds of changes Ofcom would consider to be proportionate, or where it would set the threshold for changes that may be disproportionate.[35]

3.37 The ICO also noted the draft guidance, at paragraph A6.5(b)(ii), stated that the Warning Notice would set out any proportionate changes to the service's infrastructure that may be needed to effectively implement the technology or (where a service provider is already using accredited technology) to do so more effectively, but does not clarify how Ofcom interprets the meaning of a service's "infrastructure".[36]

3.38 Some civil society respondents urged us to exercise caution when considering technical feasibility. For example, the Internet Watch Foundation (IWF) urged us to broaden our interpretation of 'technically feasible' to include innovative safety measures, rather than just measures already well-used across the industry.[37] The Marie Collins Foundation

---

[28] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.7; Charlie response to December 2024 Consultation, p.1; Name Withheld 1 response to December 2024 Consultation, p.1 ; X response to December 2024 Consultation, pp.1-2; [✂] response to December 2024 Consultation, pp.2-4; Chayn response to December 2024 Consultation, pp.5-6 and pp.8-9; Big Brother Watch response to December 2024 Consultation, pp.1-2; [✂] response to December 2024 Consultation, p.15; [✂] response to December 2024 Consultation, pp.4-5; [✂] response to December 2024 Consultation, p.2; Name withheld 3 response to December 2024 Consultation, p.1.

[29] [✂] response to December 2024 Consultation, p.2.

[30] Internet Society response to December 2024 Consultation, p.3.

[31] Internet Society response to December 2024 Consultation, p.2.

[32] [✂] response to December 2024 Consultation, p.17.

[33] [✂] response to December 2024 Consultation, p.16.

[34] [✂] response to December 2024 Consultation, p.16.

[35] ICO response to December 2024 Consultation, pp.9-10.

[36] ICO response to December 2024 Consultation, pp.9-10.

[37] IWF response to December 2024 Consultation, p.10.

encouraged us to consider options for improving the overall safety regime without undue reliance on technical feasibility arguments by providers, particularly in E2EE environments.[38] Linked to this, the NCA said that the onus should be on the provider to prove that the use of a particular technology is not technically feasible, by providing detailed rationale.[39]

3.39 The NSPCC stated it is crucial that platforms cannot avoid technology adoption on feasibility grounds alone, and that where there are no suitable accredited technologies, Ofcom's power to require services to develop their own solutions should be utilised.[40]

Our response

3.40 We note that stakeholders generally welcomed the inclusion of technical feasibility as a factor that Ofcom would consider. Our view remains that it would be appropriate for Ofcom to consider this (alongside the Specified Matters and any other matters that we consider appropriate) before issuing a Technology Notice in any particular case – and, indeed, that this would always be a consideration for Ofcom. We have therefore revised the Guidance to make clear that we will always consider this when reaching a view on whether a Technology Notice is necessary and proportionate, with some additional clarificatory changes, and moved the text to a separate paragraph 3.8 in the Guidance.

3.41 We recognise the desire from some stakeholders to have greater clarity on what technical feasibility means. However, we consider that paragraph 3.8 of the Guidance already provides adequate guidance on this matter. We note, in particular, that it refers to the "technical feasibility for the service provider of doing what would be required of them in the Technology Notice, taking into account the way the service is configured." The Guidance also makes clear, consistent with our Codes of Practice, that we may consider a solution to be technically feasible even where proportionate changes would be required to be made to the design and/or operation of the service for the technology to be used effectively.

3.42 Linked to the above, we are also satisfied that our Guidance does not narrow the scope of what may be technically feasible to measures already in industry use. For the avoidance of doubt, that is not our intention.

3.43 Having considered the ICO's comment that our draft guidance did not clarify how we interpret the term "infrastructure", we note that we have amended paragraph 6.5(b)(ii) of the Guidance so that we no longer refer to changes needed to the service's infrastructure. Consistent with section 125(5) of the Act, the paragraph instead refers to changes needed to the "design or operation" of the service.

3.44 We recognise that there are differing views among some stakeholders regarding what is technically feasible in some online spaces, particularly E2EE services. However, we do not consider that it would be appropriate to reach a view in the abstract in our Guidance about the circumstances in which it would (or would not) be technically feasible for a service to comply with the requirements of a Technology Notice. We are concerned that this would risk inappropriately fettering our discretion and note that:

[38] Marie Collins Foundation response to December 2024 Consultation, p.4.
[39] NCA response to December 2024 Consultation, pp.4-5.
[40] NSPCC response to December 2024 Consultation, p.5.

a) as explained in paragraph 3.86 below, our Technology Notice powers are intended to be broad, flexible and technology neutral. It is also clear in section 125(5) of the Act that proportionate changes to the design or operation of the service can be required by a Technology Notice;

b) whether changes required by a Technology Notice to the design or operation of a particular service are proportionate is a matter that we would need to consider on a case-by-case basis, having regard to each of the Specified Matters and any other matters that we consider appropriate to consider (see, however, paragraph 3.87 below); and

c) Ofcom's view on what changes may be proportionate (and therefore what may be technically feasible) in the context of a Technology Notice may be different to its view on what is proportionate in the context of its Codes of Practice. As noted in paragraph 2.7(d) above, Ofcom is unable to recommend the use of proactive technology on content communicated privately in its Codes of Practice, and any measures it does recommend apply to all (or particular segments of) service providers. Technology Notices however apply to a particular provider only and may require the use of technology on content communicated privately in some cases.

3.45 We have however confirmed, in response to the ICO's feedback, that we would not consider it proportionate to require changes that would undermine technical or organisational measures necessary for compliance with UK data protection law (see paragraph 3.106(b) below).

3.46 Finally, we agree that a Notice to develop or source technology may be appropriate where no suitable accredited technology currently exists, and we will consider the proportionality of imposing such a requirement on a case-by-case basis. We are satisfied that our Guidance already reflects this (see, in particular, paragraph 3.14 of the Guidance).

Size, capacity and financial cost

Summary of stakeholder responses

3.47 Stakeholders generally agreed that the financial cost to providers of complying with a Technology Notice should be considered by Ofcom before issuing such a Notice or did not comment on this. However:

a) one stakeholder invited Ofcom to consider how it can ensure that Technology Notices do not result in providers being asked to rely on technology at the expense of existing resources, noting that automated solutions require significant costs to deploy, including acquisition, operational and energy costs, which is a barrier to small and unprofitable services;[41] and

b) as noted at paragraph 3.15 above, some stakeholders expressed concern about this being given undue weight and suggested that safety should take precedence over considerations of the financial cost. In particular, the Marie Collins Foundation considered that the size and capacity of the service provider risked being "overly provider-centric", and explained that providers must absorb and comply with measures as a prerequisite for the right to do business with UK users.[42] The IWF stated that

[41] [✂] response to December 2024 Consultation, p.2.
[42] Marie Collins Foundation response to December 2024 Consultation, p.6.

potential loss of customers should not be given undue weight when assessing the financial cost of complying with a Technology Notice, and that the safety of a service must take precedence over the profit derived from creating a market that could enable illegal activities.[43]

3.48 Drs Shurson, Keenan and Ó Floinn stated that Ofcom should not only consider the proportionality of costs relative to an individual service's financial position but also the market in services. They suggested there is a real risk that "the market in UK digital services" is negatively impacted in terms of investment and innovation by the bespoke requirements of the Act, driving investment into alternative jurisdictions.[44]

Our response

3.49 We have amended the Guidance, at paragraph 3.9(b), to clarify the financial costs that we are likely to consider.

3.50 We appreciate that service providers may be concerned about the costs of complying with a Technology Notice. The Guidance therefore states, at paragraphs 3.9 (a) and (b), that we expect the size and capacity of the service provider, as well as the financial cost of complying, will be relevant to our consideration of whether it is necessary and proportionate to issue a Technology Notice. It also notes that, in accordance with section 236(1) of the Act, 'capacity' refers to both the financial resources of the service provider and the level of technical expertise available, or which it is reasonable to expect would be available, to the service provider given its size and financial resources. The Guidance further explains that, where appropriate, we would consider giving the service provider flexibility to choose between different accredited technologies in order to comply with the Technology Notice (see paragraph 3.13(d)).

3.51 However, we have amended the Guidance to make clearer that, in the case of a Technology Notice requiring the use of accredited technology, this would include having regard to the likely one-off and ongoing costs for the service provider to use the technology for the period required by the Notice (and to comply with any other specific requirements we are considering imposing), such as the price payable (see paragraph 3.9(b) of the Guidance).

3.52 We also note that one of the Specified Matters we must consider under the Act is whether the use of any less intrusive measures than the specified technology would be likely to achieve a significant reduction in the amount of terrorism or CSEA content. As we explain in the Guidance, we would therefore take into account the availability of any other tools to address our concerns when considering whether it is necessary and proportionate to issue a Technology Notice in a particular case.

3.53 On the concerns raised by the Marie Collins Foundation and the IWF, we have already explained at paragraphs 3.24 to 3.27 above why we disagree that the Guidance should require us to place greater weight on any of the particular Specified Matters or other matters we have said that we would consider. Having said that, we note that alongside the size, capacity and financial cost, we also make clear that we would expect to consider the potential impact of the Technology Notice in reducing the amount of terrorism or CSEA content on the service (paragraph 3.9(d) of the Guidance). The Guidance recognises the very substantial public interest in measures that reduce its prevalence and dissemination

[43] IWF response to December 2024 Consultation, p.7.
[44] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.8.

online, including in relation to prevention of crime and disorder, public safety, the protection of health or morals, the protection of the rights and freedoms of others and, in relation to CSEA in particular, the rights of children not to be subject to such abuse and harm together with the protection of their personal data.

3.54 Further, while we acknowledge that the costs of complying with a Technology Notice may be significant for some services – indeed, some service providers may struggle to resource the requirements we are considering imposing in a Notice and it is even possible that some may decide to cease operating their service in the UK altogether – this would not necessarily mean that the Technology Notice is not proportionate considering all the Specified Matters (where applicable) and any other factors we consider relevant in the circumstances.

3.55 It is not clear what Drs Shurson, Keenan and Ó Floinn mean by "the market in UK digital services". If they are referring to the impact on regulated service providers in general, then it is not clear to us why a Technology Notice would have a wider impact on the industry. A Notice would be issued to a particular service provider on a case-by-case basis, as emphasised in our Guidance. Any decision as to whether a Technology Notice is necessary and proportionate in a particular case would be highly fact-specific and taken in the round, taking into account the matters we must consider under the Act and any other matters or considerations that might be relevant to our assessment.

3.56 To the extent they are concerned about the impact on developers of trust and safety technology, and that Technology Notices and/or the wider online safety regime might drive investment to alternative jurisdictions, then we disagree. We expect our Technology Notice functions (and the wider online safety regime) to promote competition and growth and encourage investment and innovation in trust and safety technology in the UK. For example, as explained in our Advice to the SoS, the audit-based assessment we are recommending for the minimum standards of accuracy has been designed to be technology agnostic and to be appropriate for the vast range of different technology developers that may want to apply for accreditation. We also note that accreditation is, of course, voluntary.

3.57 Our Guidance also sets out that, when exercising our Technology Notice functions, we will act in accordance with our principal duty under section 3(1) of the Communications Act 2003 (the Communications Act). In doing so, one of the objectives we are required to secure is the adequate protection of citizens from harm presented by content on regulated services, through the appropriate use by providers of such services of systems and processes designed to reduce the risk of such harm. In our work to secure this objective, the matters we must have regard to (to the extent they appear to us relevant) include the desirability of promoting the use by providers of regulated services of technologies which are designed to reduce the risk of harm to citizens presented by content on regulated services (see paragraphs 2.31 to 2.33 of the Guidance).

Impact on other rights protected by the ECHR

Summary of stakeholder responses

3.58 Stakeholders were generally supportive of the guidance making clear that, alongside the Specified Matters (which include reference to the right under Article 8 of the ECHR to the right to a private life, and the right under Article 10 to freedom of expression within the

law), Ofcom would expect to consider the impact of a Technology Notice on other rights protected by the ECHR.

3.59 However, some stakeholders suggested that the guidance did not go far enough in recognising the impact that a Technology Notice could have on a provider's or an individual's rights. In particular:

a) Drs Shurson, Keenan and Ó Floinn explained that there is a risk of Ofcom unduly interfering with the provider's rights.[45] They suggested that requiring the compelled development of new digital technologies under penalty of law (i.e., as part of a Notice requiring the development or sourcing of technology) could be viewed as a form of compelled speech, and that code is a recognised mode of expression protected by copyright. They also explained that Technology Notices could interfere with a provider's right to conduct a business, right to property and freedom of contract, particularly if Ofcom were to require the use of its resources to develop or source technology if ultimately its use would clearly not be possible due to the risk of impact on, for example, individuals' freedom of expression and privacy; and

b) responses submitted as part of the Open Rights Group campaign, as well as one of the individual respondents, emphasised the potential adverse impacts of scanning systems on particular groups (including those with protected characteristics) and Ofcom's duties under the Equality Act 2010.[46]

Our response

3.60 Having carefully considered responses to our consultation, we have decided to amend paragraph 3.9(c) of the Guidance so that it does not focus only on rights protected by the ECHR.

3.61 Our view remains that the Guidance should acknowledge the importance of considering other rights protected by the ECHR (i.e., not just individual's rights to a private life and freedom of expression within the law, both of which are Specified Matters). Other rights that are protected by the ECHR and which could be impacted by a Technology Notice include the right to freedom of thought, conscience and religion and the right to freedom of assembly and association. However, we recognise that individuals' rights under the Equality Act 2010 (the 'Equality Act') are also important and should be considered when deciding whether it is necessary and proportionate to issue a Technology Notice (and, if so, what requirements to include).

3.62 We also acknowledge that providers may have concerns about the impact of a Technology Notice on their own rights and that, if so, this would be a relevant consideration for Ofcom. However, in line with our position at paragraph 3.66 below on conflicts of laws, we would expect the service provider to explain clearly why the issuing of a Technology Notice (and, in particular, the requirements we are considering imposing) would unduly interfere with those rights and explain how Ofcom might be able to address their concerns.

[45] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, pp.6-7.
[46] Open Rights Group's '48 hours to tell Ofcom: Practice safe text' campaign, pp.2-3; Name Withheld 2 response to December 2024 Consultation, p.1.

Conflicts of law

Summary of stakeholder responses

3.63 Some stakeholders referred to the potential for conflict of laws as another matter that Ofcom should consider. In particular:

a) Drs Shurson, Keenan and Ó Floinn suggested that Ofcom should add the potential for conflict with laws in third countries as one of the other matters we are likely to consider, noting that this would be consistent with provisions relating to Technical Capability Notices in the IPA 2016;[47]

b) [✂], X, and [✂] also said Ofcom should consider the interaction between Technology Notices and other legislative frameworks, including both the UK GDPR and laws in other jurisdictions;[48] and

c) [✂] suggested that many providers in scope of both the Act and the EU Digital Services Act (DSA) will struggle to justify automatic scanning of users' communications in light of the prohibition on general monitoring under Article 8 of the DSA.[49]

3.64 Two of these stakeholders also warned that it may be impossible for technologies to be used to target only UK users given the global nature of providers and their services. They stated this creates the potential for conflicts of law on service providers, which may result in the potential withdrawal of services from the UK market.[50]

Our response

3.65 We must consider the level of risk of the use of the specified technology resulting in a breach of privacy and data protection law when deciding whether it is necessary and proportionate to issue a Technology Notice requiring the use of accredited technology. This is one of the Specified Matters under the Act. This would include, but not be limited to, the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Paragraph 3.7(f) of the Guidance also states that we would typically expect to consider this matter in the case of a Notice to develop or source technology even though we are not required to under the Act. We discuss further feedback we received from stakeholders on data protection, and our response, from paragraph 3.99 below. This includes, for example, that where we are considering issuing a Technology Notice, we would expect this to trigger discussion between the ICO and Ofcom about how our teams may be able to collaborate and about the extent to which we may be able to share information.

3.66 We acknowledge, however, that service providers may be concerned about conflicts with their obligations under other legislative frameworks, both in the UK and other jurisdictions. We have therefore amended our Guidance to note that we will, to the extent possible, take account of any other relevant legislation which the service provider explains would restrict their ability to comply with the Technology Notice. However, we would expect the service provider to draw any such legislation to our attention and to explain why they consider the

[47] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.6.
[48] [✂] response to December 2024 Consultation, p.17; X response to December 2024 Consultation, pp.2-3 and p.6; [✂] response to December 2024 Consultation, p.4.
[49] [✂] response to December 2024 Consultation, p.3.
[50] Drs Shurson, Keenan, Ó Floinn response to Ofcom's December 2024 Consultation, p.6; [✂] response to December 2024 Consultation, p.9

legislation would restrict their ability to comply with the Notice and the requirements we are considering imposing, as well as how Ofcom might be able to address their concerns (see paragraph 3.11 of the Guidance).

3.67 For the avoidance of doubt, as paragraph 2.23 of the Guidance makes clear, Ofcom may impose requirements in a Technology Notice only in relation to the design and operation of a service in the UK, or as it affects UK users of the service.[51]

Threshold for intervention

Summary of draft guidance

3.68 Consistent with the Act, the draft guidance explained in paragraph A3.1 that Ofcom can only issue a Technology Notice where we consider it necessary and proportionate to do so. The draft guidance did not however go any further than this, for example by stating that Technology Notices will only be used as a 'last resort'.

Stakeholder responses

3.69 The Marie Collins Foundation encouraged Ofcom to be tenacious in the application of our duties and potential interventions, warning that oversensitivity to potentially intrusive measures may curtail the effectiveness of interventions, including issuing Technology Notices.[52]

3.70 In contrast, Drs Shurson, Keenan and Ó Floinn expressed concern about the risk of mission creep, explaining that without robust "red-lines" on the necessity of implementing Technology Notices they are concerned Ofcom could come under political and public pressure to justify or amend decisions in individual cases.[53] They suggested, for example, that Ofcom should be clear in the guidance that a Technology Notice is a "last resort" to be used where no other less intrusive measures have worked for a service that is otherwise not in compliance with its duties under the Act. Similarly, [✂] suggested that the guidance should acknowledge that there is a high bar for intervention, with Ofcom only using Technology Notices as a last resort where there is clear evidence of actual (rather than the potential for) harm and very material evidence of a provider having failed to address terrorism or CSEA content using their own content moderation processes first.[54] Further, some responses submitted as part of the ORG campaign emphasised the need to focus on improving law enforcement capabilities within existing legal frameworks as an alternative to using Technology Notices.[55]

Our response

3.71 We note the submissions made by some stakeholders about the circumstances and manner in which we should exercise our Technology Notice powers. However, we have decided to not make any changes to the Guidance in light of these. We are satisfied that the Guidance on which we consulted is sufficiently clear about the threshold for intervention (i.e., that we

[51] Section 125(10) of the Act.
[52] Marie Collins Foundation response to December 2024 Consultation, p.5.
[53] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.8.
[54] [✂] response to December 2024 Consultation, pp.4-5.
[55] Open Rights Group's '48 hours to tell Ofcom: Practice safe text' campaign, p.3.

may only issue a Notice where we consider it necessary and proportionate to do so taking account of each of the Specified Matters), and is consistent with the statutory framework.

3.72 We note the concern raised by one stakeholder that Ofcom should not issue a Technology Notice unless there is clear evidence of actual (rather than the potential for) harm and evidence that the provider has failed to address terrorism or CSEA content using its own content moderation processes first. Some of the Specified Matters require Ofcom to consider evidence of actual harm (see, for example, sections 124(2)(d) and (e) of the Act) and the provider's existing systems and processes (see, in particular, section 124(2)(g) and paragraph 3.20 above). However, section 124(2)(f) is clear that consideration of the Specified Matters may include the risk of harm. As such, we do not consider that the Guidance should be amended.

3.73 Finally, we recognise the value of wider safety-by-design measures when it comes to preventing the occurrence of harmful activity and to empower users to keep themselves safe if they encounter such activity. Our Technology Notice powers are necessarily focused on the use, development or sourcing of technology to deal with terrorism/CSEA content. However, paragraph 3.7(e) and section 4 of the Guidance make clear that Technology Notices are just one of our regulatory powers available to tackle terrorism and CSEA content, and we recognise the wider remit of our Codes of Practice and focus in our Codes on safety-by-design measures. As explained in the Guidance, we would take the availability of these other tools into account when considering whether it is necessary and proportionate to issue a Technology Notice in a particular case. For completeness, and while we acknowledge the importance of law enforcement to stopping the spread of CSEA and terrorism propaganda both online and offline, we note that Ofcom has no role in criminal law enforcement and that this is not a matter that we would consider when deciding whether it is necessary and proportionate to issue a Technology Notice in a particular case.

Fundamental Rights Impacts

Summary of draft guidance

3.74 There was no specific sub-section on fundamental rights impacts in the draft guidance. However, paragraph A3.6 of the draft guidance explained that, where we are considering requiring the use of accredited technology, we must have regard to certain matters including:

a) the level of risk of the use of the specified technology resulting in a breach of any statutory provision or rule of law concerning privacy; and

b) the extent to which the use of the specified technology would or might:

i) result in interference with users' rights to freedom of expression within the law; and

ii) have an adverse impact on the availability of journalistic content on the service or result in a breach of the confidentiality of journalistic sources.

3.75 Paragraph A3.7(f) also explained that, while we are not required to consider these matters in the case of a Notice to develop or source technology, we would typically expect to do so.

3.76 The draft guidance also stated that we must consider whether the use of any less intrusive measure would be likely to result in a significant reduction in the amount of relevant content.

3.77 Further, paragraph A3.8 set out other matters that we are likely to consider. These included the technical feasibility for the provider of doing what would be required by the Technology Notice (taking into account the way the service is configured), and the impact on other rights protected by the ECHR.

End-to-end encryption (E2EE)

Summary of stakeholder responses

3.78 We did not discuss the powers to issue a Technology Notice in relation to E2EE services in the draft guidance. A number of stakeholders raised comments in relation to how our draft guidance and use of this power could impact E2EE services.

3.79 On the one hand, many stakeholders noted the benefits of encryption and the potentially significant risks associated with weakening encryption, which they considered may arise if Ofcom were to issue a Technology Notice to an E2EE service. Such benefits and risks raised by stakeholders can be broadly characterised as follows:

a) the benefits that E2EE communications afford to users in protecting their data, privacy, freedom of expression and association. Most respondents underlined the importance of private communications for everybody, while some stakeholders emphasised benefits to individuals with protected characteristics (e.g., women, children, LGBTQIA+ individuals, individuals with disabilities) or vulnerable populations (e.g., domestic abuse survivors, people in care, individuals experiencing tech-facilitated abuse), as well as academics, activists, and journalists.[56] Stakeholders also referred to the benefits for protecting the security and privacy of communications, and helping to protect users against various threats including hacking, identity theft, and unauthorised access to sensitive information;[57]

b) the risk that any weakening introduced to an E2EE system could pose serious unintended consequences for users.[58] The Open Rights Group, Big Brother Watch, the Internet Society, X, Chayn, [✂] and many individual respondents told us that any requirement to scan E2EE content acts as a functional "backdoor" that could be exploited by bad actors and undermines the security and privacy of all users. These respondents argued that any measures requiring scanning of encrypted content would necessarily involve weakening or circumventing encryption.[59] Some of the responses to

[56] Chayn response to December 2024 Consultation, p.4 and pp.6-7; Big Brother Watch response to December 2024 Consultation, pp.3-4; Charlie response to December 2024 Consultation, p.1; [✂] response to December 2024 Consultation, p.2; Open Rights Group's '48 hours to tell Ofcom: Practice safe text' campaign, pp.2-3.
[57] Big Brother Watch response to December 2024 Consultation, pp.3-4; [✂] response to December 2024 Consultation, p.15; Internet Society response to December 2024 Consultation, pp.2-3; Name Withheld 1 response to December 2024 Consultation, p.1; [✂] response to December 2024 Consultation, p.2; Chayn response to December 2024 Consultation, pp.5-6
[58] [✂] response to December 2024 Consultation, pp.2-3.
[59] Open Rights Group response to December 2024 Consultation, pp.1-2 and p.4; Big Brother Watch response to December 2024 Consultation, pp.4-6; Internet Society response to December 2024 Consultation, pp.3-4; X response to December 2024 Consultation, p.2; Chayn response to December 2024 Consultation, pp.2-3 and p.8; [✂] response to December 2024 Consultation, pp.2-3; [✂] response to December 2024 Consultation,

the Open Rights Group's campaign further noted this may result in a weakening of public trust in secure communications, financial and business transactions;[60]

c) Drs Shurson, Keenan and Floinn noted that computer scientists have warned of systemic risks in uses of technology that circumvent E2EE communications and have called for rigorous public review and testing before any consideration is given to mandating its use;[61] and

d) the risk that E2EE service providers may discontinue their offering in the UK, resulting in less consumer choice.[62] One stakeholder specifically requested that Ofcom clarify in its final guidance that it would not use these powers to order companies to scan encrypted content, warning that without such clarification, certain providers may discontinue offering their services in the UK or provide only limited offerings.[63]

3.80 On the other hand, a number of other stakeholders - particularly child safety organisations - pointed to the safety risks posed by E2EE services in enabling perpetrators to spread CSEA content and supported the use of the Technology Notices powers to address CSEA content in E2EE environments.[64] The NSPCC noted that CSEA can take various forms, and can occur across various platforms including on E2EE services, and this range of risks and platforms underlines the need for a variety of recognised technological solutions that can mitigate the risks.[65]

3.81 Some stakeholders also expressed views regarding the limitations of the power itself with regard to such services:

a) some suggested that Ofcom cannot issue a Notice to the provider of an E2EE service. For example, [✂] stated that Ofcom should clarify in the guidance that the presence of E2EE is a factor that would preclude it from issuing a Technology Notice.[66] Similarly, X sought confirmation that E2EE services will not be subject to Technology Notices.[67] The Internet Society noted that Technology Notices issued to E2EE services would be open to challenge on the basis that they would constitute a disproportionate interference with privacy rights;[68] and

---

pp.3 and pp.15-16; Name Withheld 1 response to December 2024 Consultation, p.1; Name Withheld 2 response to December 2024 Consultation, p.1; Name Withheld 3 response to December 2024 Consultation, p.1; Name Withheld 4 response to December 2024 Consultation, p.1; Name Withheld 5 response to December 2024 Consultation, p.1; Charlie response to December 2024 Consultation, p.1; Open Rights Group's '48 hours to tell Ofcom: Practice safe text' campaign, pp. 2-3.

[60] Open Rights Group's '48 hours to tell Ofcom: Practice safe text' campaign, p.4.

[61] Drs Shurson, Kennan, Ó Floinn response to December 2024 Consultation, pp.5-6.

[62] Open Rights Group response to December 2024 Consultation, p.4; Name Withheld 1 response to December 2024 Consultation, p.2; Name Withheld 2 response to December 2024 Consultation, p.1; Name Withheld 3 response to December 2024 Consultation, p.1; Name Withheld 4 response to December 2024 Consultation, p.1; Name Withheld 5 response to December 2024 Consultation, p.1; [✂] response to December 2024 Consultation, pp.4-5; Open Rights Group's '48 hours to tell Ofcom: Practice safe text' campaign, pp. 2-3.

[63] [✂] response to December 2024 Consultation, pp.4-5.

[64] IWF response to December 2024 Consultation, pp.1 and 6; Marie Collins Foundation response to December 2024 Consultation, p.4;

[65] NSPCC response to December 2024 Consultation, p.1.

[66] [✂] response to December 2024 Consultation, p.3

[67] X response to December 2024 Consultation, p.1 and pp.5-6.

[68] Internet Society response to December 2024 Consultation, p.2 and p.7.

b) many stakeholders suggested that even if Ofcom has the power to issue a Technology Notice in relation to an E2EE service, it would not be necessary and proportionate to do so where the Notice requires:

i) the removal or weakening of encryption. Multiple stakeholders suggested that Ofcom should provide clarity in the guidance that Technology Notices should not mandate any technologies that will undermine or compromise E2EE and therefore the privacy and freedom of expression of users;[69] and

ii) the use of what some stakeholders referred to as 'client-side scanning' technologies. Stakeholders raised several specific concerns about requiring scanning of encrypted communications. These included undermining the security model of E2EE services, which would create vulnerabilities that could be exploited by malicious actors;[70] that it would impact users' privacy;[71] that it would not be technically feasible to limit scanning only to UK users, meaning that global services would need to implement changes affecting all users worldwide; [72] and that this could place providers in conflict with regulatory requirements in other jurisdictions that protect or mandate encryption.[73]

3.82 However, while many stakeholders were concerned about the use of 'client-side scanning' technologies, we also heard from other stakeholders - the Marie Collins Foundation and the IWF – who encouraged Ofcom to consider such technologies, noting that such solutions exist and are deployed by some regulated services already.[74] The IWF asked Ofcom to reject any assertions that `client-side scanning', pre-screening or upload prevention "breaks encryption", stating in their opinion this is not technically correct.[75]

3.83 We heard from a provider of E2EE services who suggested that consideration of wider safety-by-design measures are important – "*ranging from those which aim to prevent the occurrence of harmful activity in the first place, to those that empower users to keep themselves safe if they encounter such activity*" - and, in their view, can be grounded in international human rights law.[76]

---

[69] Drs Shurson, Kennan, Ó Floinn response to December 2024 Consultation, pp.4-5; Charlie response to December 2024 Consultation, p.1; Name Withheld 1 response to December 2024 Consultation, p.2; X response to December 2024 Consultation, pp.1-2; Chayn response to December 2024 Consultation, pp.5-6 and pp.8-9; Big Brother Watch, response to December 2024 Consultation, pp.1-2; [✂] response to December 2024 Consultation, pp.3 and pp.15-16; [✂] response to December 2024 Consultation, pp.4-5; [✂] response to December 2024 Consultation, p.2; Internet Society response to December 2024 Consultation, pp.1 and pp.6-7; Name withheld 3 response to December 2024 Consultation, p.1.

[70] Open Rights Group response to December 2024 Consultation, pp.1-4; Open Rights Group's '48 hours to tell Ofcom: Practice safe text' campaign, pp.1-2; Internet Society response to Ofcom's December 2024 Consultation, pp.1 and pp.3-5; Big Brother Watch, response to December 2024 Consultation, pp.4-5

[71] Big Brother Watch, response to December 2024 Consultation, pp.2-4; X response to December 2024 Consultation, pp.1-2

[72] Internet Society response to Ofcom's December 2024 Consultation, p.7.

[73] Internet Society response to Ofcom's December 2024 Consultation, p.7. X response to December 2024 Consultation, p.3

[74] Marie Collins Foundation response to December 2024 Consultation, p.4; IWF response to December 2024 Consultation, p.2 and pp.7-8.

[75] IWF response to December 2024 Consultation, pp.7-8.

[76] [✂] response to Ofcom's December 2024 Consultation, p.3.

Our response

3.84 We have carefully considered all of the consultation responses regarding E2EE and recognise that this is an important theme raised by many respondents (often with polarised views). As we explain below, we are not persuaded that changes are required to our Guidance on these matters.

3.85 We recognise that E2EE affords certain benefits, as noted in paragraph 3.79(a) above, for the security and privacy of communications. However, notwithstanding its benefits, Ofcom remains of the view that encryption (particularly E2EE) is a risk factor for certain harms. This includes terrorism and CSEA harms and these risks were raised by several respondents to our consultation. The risks of E2EE are reflected in our Register of Risks (see for example paragraphs 1.51 to 1.54; 2A.9 to 2A.11; and 2B.67 to 2B.69).

3.86 We do not agree with the statement from some stakeholders that Ofcom does not have the legal power to issue a Technology Notice to an E2EE service. The Act contains no such direct prohibition or limit on Ofcom's powers, which under section 121 of the Act are intended to be broad, flexible and technology neutral. Further, the fact that content is itself encrypted does not mean that associated data and information (such as user data and metadata) is encrypted.

3.87 Whether there are circumstances under which it will ever be necessary and proportionate to issue a Technology Notice in relation to an E2EE service will depend on the specific circumstances. Both the benefits afforded by E2EE services and the risks for certain harms would need to be carefully considered as part of any assessment of whether to issue a Technology Notice and, if so, what requirements to include. Our role is to implement the powers we have been given under the Act (including to tackle terrorism and CSEA content online) in a way that is proportionate and compatible with fundamental rights. This requires us to make careful, evidence-based assessments in each case about whether the statutory tests are met. Technology Notices can be issued in relation to terrorism and CSEA content only where we consider it necessary and proportionate, and subject to significant procedural and substantive requirements set out in the Act and reflected in our Guidance. With regard to the two specific scenarios raised by stakeholders at 3.81(b)(i) and (ii) above:

a) on the removal or weakening of encryption: the Act clearly envisages in s125(5) that some changes may be required to a regulated service in order for it to comply with a Technology Notice. However, as noted in the Explanatory Notes to the Act, and in our Guidance, these changes are expected to be proportionate. Further, any Technology Notice itself must be necessary and proportionate, taking account of each of the Specified Matters (which include impacts on freedom of expression and privacy). Whether specific changes are proportionate will need to be considered on a case-by-case basis, and it is not necessary or appropriate in our view for our Guidance to seek to specify in advance what may or may not be necessary and proportionate in particular circumstances; and

b) on the requirement to use what stakeholders have referred to as ‘client-side scanning’: we are satisfied that the Act provides us with a broad power to require the providers of regulated services to use accredited technology, including to prevent users encountering content (and therefore before that content is communicated by means of the internet service). We therefore disagree with the arguments that Ofcom does not have the power to require the use or development/sourcing of such technology, or that it could never be necessary and proportionate for Ofcom to require this. However,

whether it is necessary and proportionate will depend on the specific circumstances, and we have not taken (nor do we consider that it would be appropriate to take) a view on whether technology currently exists that could be used on content before it is uploaded without unduly interfering with users' fundamental rights. Further, some key considerations to bear in mind with such scanning are that:

i) Ofcom does not have the power to compel persons other than the providers of regulated services to deploy such technology (for example, Ofcom has no powers under section 121 in respect of device manufacturers);

ii) Ofcom would need to consider other laws such as the PECR, which contain specific provision about the accessing and storage of information on terminal equipment such as mobile devices; and

iii) while there has been some disagreement amongst respondents on whether such scanning 'undermines' or 'breaks' encryption, such technology would result in the monitoring of content on users' own devices and would therefore amount to a significant interference with users' rights to privacy and freedom of expression. When considering whether the deployment of such technology may be necessary and proportionate, these are factors we are required by the Act to particularly consider.

3.88 As noted at paragraph 3.73 above, we recognise the value of wider safety-by-design measures. Our Guidance makes clear that Technology Notices are just one of our regulatory powers available to tackle terrorism and CSEA content, recognising the wider remit of our Codes of Practice and focus in our Codes on safety-by-design measures.

3.89 Finally and for completeness, we note that it will remain the case that, if law enforcement wants specific information about a specific individual, to intercept communications, or to obtain communications data, then they would still need to do so using powers under (and accordance with) the Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016, as appropriate.

Freedom of Expression and right to privacy

Summary of stakeholder responses

3.90 One stakeholder strongly urged Ofcom to consider the disproportionate impact of technologies on individuals' rights, including freedom of expression and the right to privacy under the Human Rights Act 1998. In particular, they were concerned about the risk of detection technologies misidentifying private information as terrorism content and, without oversight, the potential for false accusations against innocent users with serious real-world consequences and harming already marginalised groups and further entrench existing inequalities.[77]

3.91 The Internet Society were concerned that accuracy thresholds that may appear high would still result in millions, if not billions, of false positives given the volume of messages sent daily, with such cases potentially being blocked, subjected to invasive human review or forwarded to third parties, such as law enforcement or safety agencies.[78]

[77] [✂] response to December 2024 Consultation, pp.3-4.
[78] Internet Society response to December 2024 Consultation, p.1 and p.7.

3.92 Another stakeholder stated that Ofcom should set out more detail regarding how its requirement to consider freedom of expression and privacy as part of the Specified Matters interacts with its own duties under the Human Rights Act 1998, including practical examples of how these considerations might influence Ofcom in practice.[79]

3.93 Similarly, a stakeholder sought acknowledgment in the guidance that the use of the power to issue a Technology Notice in respect of content communicated privately would constitute a serious interference with users' expectations and rights to privacy.[80]

3.94 Another stakeholder noted that safeguarding freedom of expression and privacy within the Act is a key priority for services and sought clarity in the guidance as to how services can maintain and uphold principles such as freedom of expression and privacy in accordance with human rights law.[81]

Our response

3.95 We recognise the potentially significant impacts the use of terrorism and/or CSEA content detection technologies in practice could have on users' rights, including to freedom of expression and to privacy. However, we are not persuaded changes are required to our Guidance.

3.96 The Specified Matters we are required to have particular regard to under the Act, in the case of a Notice requiring the use of accredited technology, include the potential impact on user's rights to freedom of expression and privacy. Our Guidance explains that, while not required by the Act, we would typically expect to also consider those matters in the case of a Notice to develop or source technology (this is discussed further in paragraph 3.116 below). Any Technology Notice, and the specific requirements we decide to include, would therefore be designed with these matters in mind. We further note that our Guidance:

a) acknowledges the risk of users incorrectly having their content removed, account banned or suspended, or being reported to the NCA or other organisations and that this would represent a potentially significant impact on their rights to freedom of expression and privacy. It explains that we would therefore expect to have regard to evidence regarding the false positive rate of technology under consideration when considering the extent of any anticipated interference with such rights alongside any other relevant information, for example, any potential safeguards to mitigate the risk, such as the layering of measures (see paragraph 3.7(c));

b) explains we would expect any impact on other rights protected by the ECHR to be relevant to our consideration of whether it is necessary and proportionate to issue a Technology Notice. This may include, for example, the right to freedom of thought, conscience and religion (Article 9) and to freedom of assembly and association (Article 11) (see paragraph 3.8(d))). As explained at paragraph 3.61 above, we recognise that individuals' rights under the Equality Act are also important and should likewise be considered and we have decided to amend the Guidance so that it does not only focus on rights protected by the ECHR;

c) sets out that when considering a technology's false positive rate, we would also expect to consider the nature of the content that is incorrectly detected by the technology as

[79] [✂] response to December 2024 Consultation, p.17.
[80] [✂] response to December 2024 Consultation, p.4.
[81] [✂] response to December 2024 Consultation, p.4.

terrorism or CSEA content, and one of the examples provided is whether it is afforded a greater degree of protection by the law (such as political speech); and

d) notes, at paragraph 2.37, that as a public authority Ofcom is required by section 6 of the Human Rights Act 1998 to act in a way that is compatible with the ECHR and any interference with an individual's rights needs to be justified. While we note the request for further detail, including practical examples, about how these considerations might influence Ofcom in practice, we have already explained that we do not consider that it is necessary or appropriate for the Guidance to include such examples at this stage (see further at paragraph 3.27 above).

3.97 In relation to a stakeholder's concern about the risk of private information being misidentified as terrorism content, we note that, in the case of terrorism content, our powers to issue a Technology Notice are limited to requiring the use of accredited technology on content communicated publicly.

3.98 We also acknowledge the request from another stakeholder for further guidance on how providers themselves can act in accordance with human rights law. However, in line with section 127 of the Act, the Guidance is intended only to provide procedural guidance regarding the steps Ofcom would expect to take, and the matters we would expect to consider, when exercising (or deciding whether to exercise) our Technology Notice functions.

Data protection

Summary of stakeholder responses

3.99 The ICO[82] noted that the technologies in scope of a Technology Notice will involve the processing of personal information, including in some cases the accessing or storage of information on a user's device. They suggested that the guidance should explicitly inform companies that personal information processing must fully comply with data protection law (which, in the case of storage and access technologies, includes PECR), to make clear they cannot avoid their data protection obligations merely because such processing is required to comply with a Notice.

3.100 The ICO also stated that it was particularly keen for the guidance to confirm that requiring a company to undermine or reduce technical or organisational measures that are necessary to comply with data protection law would not be considered a proportionate change to the design and/or operation of a service for the technology to be used effectively.[83]

3.101 The ICO also said we should make clear when we expect to consult it prior to issuing a Warning Notice or a Technology Notice to mitigate the risk of a breach of data protection law.[84] Drs Shurson, Keenan and Ó Floinn similarly suggested that the views of the ICO on data protection and privacy should be incorporated into decisions on whether to issue a Notice, also noting that there is no reason Ofcom could not consult with other stakeholders or experts on privacy or human rights.[85]

[82] ICO response to December 2024 Consultation, p.2 and p.9.
[83] ICO response to December 2024 Consultation, pp.9-10.
[84] ICO response to December 2024 Consultation, p.9.
[85] Drs Shurson, Keenan, Ó Floinn, response to December 2024 Consultation, p.10.

3.102 Another stakeholder explained that, as detection technologies must be applied to all customers on a particular service, they likely result in the collection of more information than is necessary to achieve the intended purposes and place providers in conflict of their obligations to ensure data minimisation and storage limitation. They also stated that it is difficult for detection technologies to explain how they have come to a result, making it difficult for providers to satisfy transparency obligations.[86]

Our response

3.103 We have carefully considered the feedback provided about the interaction between Technology Notices and data protection law. We have decided to make some changes to the Guidance in light of stakeholder feedback which we discuss below.

3.104 We acknowledge the concerns raised by some respondents about the risks of using accredited technologies on users' personal data. Ofcom is not the data protection regulator; the relevant regulator is the ICO. However, we are required to consider the level of risk of a Technology Notice requiring the use of accredited technology resulting in a breach of data protection data rules when deciding whether it is necessary and proportionate to issue a Notice in a particular case. We also recognise the value of engagement with the ICO more generally across our online safety work.

3.105 Indeed, we published a joint statement in 2022 setting out our shared vision for a clear and coherent regulatory landscape for online services, ensuring compliance with both our regimes.[87] We then issued a further statement in 2024 which builds upon that vision by setting out in more detail how we will collaborate where we identify cross-cutting online safety and data protection issues and opportunities in our regulation of specific services.[88]

3.106 We recognise the importance of ensuring that Technology Notices do not require providers to act in breach of data protection law, and the importance of accredited technology being deployed in accordance with data protection law. For this reason:

a) we have amended paragraph 2.13 of the Guidance to make clear that where a service provider is using content detection technologies (including when required to do so by a Technology Notice), they must also comply with the requirements of data protection law. We have also added a link to relevant guidance published by the ICO on PECR alongside other ICO guidance that was already referenced (i.e., the ICO guidance on content moderation and content detection);[89]

b) we would not consider it proportionate to require changes that would undermine technical or organisational measures necessary for compliance with UK data protection law. We do not however consider it necessary to amend our Guidance in this regard; and

c) we have explained at paragraph 2.13 of our Guidance that, where we are considering issuing a Technology Notice, we would expect this to trigger discussion between the ICO and Ofcom about how our teams may be able to collaborate and about the extent to which we may be able to share information. Our Guidance explains that we would generally expect such engagement to commence before we issue a Warning Notice.

---

[86] [✂] response to December 2024 Consultation, pp.3-4.
[87] Online safety and data protection: A joint statement by Ofcom and the ICO (25 November 2022)
[88] Online safety and data protection: A Joint Statement by Ofcom and the ICO (1 May 2024)
[89] The ICO has confirmed that it also intends to produce guidance on the use of behaviour identification and user profiling in the future.

This is consistent with the 2024 joint statement (referenced above), which recognises that the use of proactive technology and relevant AI tools is a 'Collaboration theme' (i.e., an issue of common interest and relevance to both Ofcom and the ICO). We are not however persuaded that our Guidance should be more prescriptive about the extent of our engagement with the ICO, as this will need to be considered on a case-by-case basis.

3.107 One respondent appeared to suggest that the use of accredited technologies will (if they require analysis of all users' content) necessarily result in a breach of data protection law. Insofar as this was the point being made by the respondent, we disagree that this is the case. As noted above, and reflected in our Guidance, the ICO has produced helpful guidance which considers how services can comply with data minimisation and other data protection principles when deploying content moderation technology.[90]

Technology Notices to develop or source technology

Summary of draft guidance

3.108 Paragraph A3.7(f) of the draft guidance stated that in the case of a Technology Notice to develop or source technology, while we are not required to consider the matters set out at paragraph A3.6 (concerning impacts on freedom of expression, privacy and availability of journalistic content and whether less intrusive measure would be effective), we would typically expect to do so.

3.109 Paragraph A3.12 of the draft guidance stated that it is more likely Ofcom would consider it necessary and proportionate to issue a Technology Notice to develop or source technology where a Notice to use accredited technology is not an option. This could be because there are no relevant accredited technologies or, where there are, it would not be technically feasible for any of those technologies to be used on the service.

3.110 Paragraph A3.13 of the draft guidance stated that when reaching a view on whether to issue a Technology Notice and the requirements to be imposed on a service, we expect to follow the process described in sections 4 to 6 of the guidance including obtaining a skilled person's report and giving the service provider the opportunity to make representations. Paragraph A7.13 of the guidance however explained that, when issuing a further Notice, we are not required to obtain a further skilled person's report or issue a further Warning Notice.

Summary of stakeholder responses

3.111 Drs Shurson, Keenan and Ó Floinn argued that we should adopt a stronger position at paragraph A3.7(f) of the draft guidance, suggesting that the impact on fundamental rights must always be considered before issuing a Notice to develop or source technology.[91] In particular, they warned there was a risk of Ofcom being exposed to liability under section 6(1) of the Human Rights Act 1998 were any developed or sourced technology to prove to

[90] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-safety-and-data-protection/content-moderation-and-data-protection/how-do-we-ensure-data-minimisation-in-our-content-moderation/

[91] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, pp.2-3.

interfere significantly with individuals' human rights if utilised by the provider (even if not legally compelled to do so by Ofcom).[92]

3.112 They further suggested the guidance should clarify that there is no obligation on the provider to use any developed or sourced technology.[93]

3.113 Similarly, while the ICO welcomed our proposed approach, they felt that, given the potential risks to user's data protection rights, it would be appropriate for Ofcom to carry out an updated assessment of the Specified Matters against the technology that is developed or sourced at the point of requiring its deployment, noting that the draft guidance did not guarantee this. [94]

3.114 Another stakeholder asked Ofcom to avoid requiring services to select a technology from a provided list when no listed options have been designed or proven effective for the services' functionalities and to allow services to create bespoke mitigations provided, they can prove the technology is as effective as the listed options. [95]

Our response

3.115 Having considered stakeholders' responses, we have decided to make some modifications to the Guidance for the reasons set out below.

3.116 Notwithstanding the suggestion that we should adopt a stronger position at paragraph 3.7(f) of the Guidance, we have decided to retain the text on which we consulted and do not consider that it would be appropriate for our guidance to go further. The Guidance makes clear that, while we are not required to consider the matters set out in paragraph 3.6 (i.e., impact on freedom of expression, privacy and journalistic content) when deciding if it is necessary and proportionate to issue a Notice regarding the development/sourcing of technology, we would typically expect to do so. Further, our view remains that the extent to which we will be able to thoroughly consider these impacts may be limited by the fact that – when considering the impacts of such a Notice – there will not be a specific technological solution in mind at that stage. We are keen for our Guidance to be clear about this.

3.117 We recognise however that there is value in the Guidance making clear that a Notice to develop or source technology does not require that any technology which is subsequently developed or sourced must then be used. A provider is only required by such a Notice to use its best endeavours to develop or source technology that meets the minimum standards of accuracy. If Ofcom considers it necessary and proportionate for that provider to then use that technology, we would expect to consider requiring this through a further Technology Notice under section 121(2)(a) or (3)(a). Before doing so, we would need to consider each of the Specified Matters (and any other matters that we consider are relevant) in line with the Guidance. We have sought to make this clear in paragraph 6.5(b)(i) of the Guidance.

3.118 We have also amended paragraph 3.15 of the Guidance to state that, where we intend to issue a further Notice (i.e., requiring a provider to use the developed/sourced technology) the process that we expect to follow is set out in paragraphs 7.12 and 7.13 of the Guidance. We are not persuaded that it will always be necessary and proportionate to obtain a skilled

[92] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, pp.2-3.
[93] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.3.
[94] ICO response to December 2024 Consultation, p.11.
[95] [✂] response to December 2024 Consultation, p.2.

person's report in such a case. However, we have amended paragraph 7.13 to make clear that we will issue a Warning Notice.

3.119 We note the concern raised that Ofcom should not require providers to use particular technologies from a list when no listed options have been designed or proven effective for its services' functionalities. However, we do not consider that further amendments are required to our Guidance in this regard and consider that the Act and draft guidance are already consistent with this. In particular, Ofcom has been given the power to issue Notices requiring the development/sourcing of technology precisely because there may be circumstances where a Notice to use accredited technology is not an option and it may be more appropriate for the provider to develop or source its own bespoke mitigation. Our Guidance also reflects this at paragraphs 3.13 to 3.14.

Compatibility testing[96]

Summary of draft guidance

3.120 The draft guidance stated that Ofcom would consider whether compatibility testing is appropriate to inform our view and set out the matters we would expect to have regard to when considering whether such testing is appropriate (paragraph A3.14).

3.121 It further explained that the timing of any testing would depend on the circumstances, but that we expect it would generally occur before we decide whether to issue a Warning Notice (paragraph A3.18).

Summary of stakeholder responses

3.122 While the ICO welcomed our proposal to consider compatibility testing (see paragraph 3.3 above), they suggested there should be a presumption that it will be carried out unless independent and robust evidence is already available about the performance of the technology for the specific use case.[97] They explained that compatibility testing could surface issues of potential breaches of data protection law which could be mitigated in the Warning Notice or Technology Notice, and enable the real-world application, as well as the potential limitations and risks, of the technology to be considered before a final decision is taken. The ICO also noted that it is their understanding that, once a technology becomes accredited, a Technology Notice can be issued without any mandatory requirement for its accuracy to be further assessed.[98]

3.123 Google and [✂] sought clarity on when compatibility testing may be required and how Ofcom will determine that it is necessary,[99] including practical examples.[100]

3.124 Stakeholders raised points on the timing and sequencing of compatibility testing:

a) [✂] considered this was unclear in the draft guidance and subject to significant discretion. They suggested that the guidance should specify that testing "must" occur before a Warning Notice, with the potential for further testing after a Warning Notice

[96] Previously termed 'independent compatibility testing' in the draft guidance.
[97] ICO response to December 2024 Consultation, p.11.
[98] ICO response to December 2024 Consultation, pp.3-4.
[99] Google response to December 2024 Consultation, p.14; [✂] response to December 2024 Consultation, p.17.
[100] [✂] response to December 2024 Consultation, p.17.

and provider representations, to ensure providers can make properly informed representations on the compatibility of any technology;[101] and

b) in contrast, Google warned that such testing would be onerous for providers, presenting a series of technical, security, legal and governance challenges. They suggested that Ofcom should only be able to require it after we have determined that issuing a Notice will be necessary and proportionate, to avoid "subjecting service providers to indefinite and unbounded testing prior to any legal conclusion that their content architecture is deficient" under the Act.[102]

Our response

3.125 We have reflected on our draft guidance and decided to make some changes, which we set out below.

3.126 We do not consider it appropriate to include a presumption in the Guidance that compatibility testing will be carried out. While we generally expect to conduct compatibility testing, the Guidance is intended to be flexible to allow us to consider in the individual circumstances whether it is appropriate to conduct such testing (including, the timing and its extent) and such a presumption could undermine this.

3.127 The Guidance already sets out the matters we would expect to have regard to in considering whether compatibility testing is appropriate at paragraph 3.16, which includes the extent to which there is independent and robust evidence available to Ofcom about the performance of the technology in question, and the relevance of that evidence to the specific use case in question. It also explains, at paragraph 5.13, that we may request that the skilled person suggest any testing that Ofcom may undertake when we are considering whether to issue a Notice. We further note that the specific service(s), technology(s) and nature of the concerns we are considering in a particular case will be highly fact specific. As such, we do not think it is necessary or appropriate to provide any further clarification on when, or how, we will determine whether compatibility testing is appropriate, or to include specific examples of when compatibility testing might be appropriate.

3.128 We are also not persuaded that the Guidance should state that compatibility testing "must" take place before a Warning Notice is issued. The Guidance is clear, at paragraph 3.20, that we expect any such testing would generally occur before we decide whether to issue a Warning Notice. However, we think it is important that the Guidance retains flexibility regarding the timing because, as it says, we might consider it appropriate to also conduct compatibility testing following representations from the provider in response to a Warning Notice. We therefore think that the current drafting strikes the right balance and reflects that the timing of any compatibility testing will depend on the circumstances of each case.

3.129 To the extent we conduct any further testing after we have issued a Warning Notice, we will give the service provider the opportunity to review the results and make any further representations before we decide whether to issue a Notice.

3.130 We disagree with Google's suggestion that Ofcom should only be able to require compatibility testing after we have determined that issuing a Technology Notice will be necessary and proportionate. The purpose of such testing would be to inform our

[101] [✂] response to December 2024 Consultation, p.6.
[102] Google response to December 2024 Consultation, pp.14-15.

assessment of whether it is necessary and proportionate to give a Notice, and the specific requirements that might be imposed.

3.131 However, we do acknowledge Google's concern that compatibility testing may be onerous for service providers. Ofcom is, however, required to exercise its information gathering powers in a way that is proportionate to the use to which the information is to be put.[103] We also note that compatibility testing might ultimately save costs and resources for the service provider, particularly if it helped to identify that it was not proportionate to issue a Notice.

3.132 We also note that some stakeholders requested more clarity about how Ofcom would consider the effectiveness of providers' existing systems and processes (see, for example, paragraph 3.10 to 3.13 above). We have, therefore, made some amendments to paragraphs 3.16 to 3.20 of the Guidance to:

a) make clear that the extent of any compatibility testing is a matter that we may request the skilled person to provide a view on as part of its report (in line with paragraph 5.13 of the Guidance);

b) add that where, for example, we consider some initial testing may be appropriate to ascertain whether there may be suitable accredited technology for the use case in question, this might also consider (if so) how it might be deployed alongside the providers' existing systems and processes;

c) clarify that, where Ofcom decides more detailed compatibility testing is appropriate:

   i) the relevant technology may be tested against one or more datasets representative of content it would expect to encounter on the service in question and not that any testing would necessarily always be against more than one dataset; and

   ii) if the provider in question already deploys technology to detect terrorism or CSEA content (or is in the process of developing such technology), this testing could also – or in the alternative – include similar testing of the provider's own technology with a view to identifying, for example, whether it may be more appropriate to issue a Notice to develop or source technology; and

d) refer to section 4 of our Online Safety Information Powers Guidance, which provides more detail on the types of considerations to which Ofcom may have regard when requiring the performance of tests as part of a notice under section 100 of the Act.

Specific requirements of a Technology Notice

Summary of draft guidance

3.133 Paragraph A3.11 of the draft guidance stated that the specific requirements that are necessary and proportionate may vary between Technology Notices.

3.134 In the case of a Notice requiring the use of accredited technology, the draft guidance noted that Ofcom would carefully consider (amongst other things) what kinds of content should be analysed. It noted that, while we have the power to require the use of accredited technology on content communicated publicly (in the case of terrorism content) and

[103] Section 100(4) of the Act.

content communicated publicly and privately (in the case of CSEA content), we would not necessarily require the use of accredited technology on all such content.

3.135 The draft guidance also noted that we would also consider the wider systems and processes that might be appropriate in each case (including, for example, the extent to which there should be human moderation).

Summary of stakeholder responses

3.136 A stakeholder sought clarification on our draft guidance that "we would not necessarily require the use of accredited technology on all such content", suggesting in particular that we add further detail on how we will take into account proportionality and our duties under the Human Rights Act 1998 and the types of scenarios in which we might require the use of accredited technology on privately communicated data.[104]

3.137 Another stakeholder stated that the draft guidance suggested accredited technology could be mandated on any part of the service. It asserted that the guidance should be clear that a Technology Notice requiring the use of accredited technology can only apply to the parts and functionalities of a service on which there is evidence relevant content (i.e., terrorism or CSEA content) is being communicated.[105]

3.138 They also suggested, in relation to the wider systems and processes that might be proportionate, that we should clarify that a Technology Notice would not require the provision of a "bespoke or duplicative" complaints procedure in addition to the complaints process already required by the Act.[106]

Our response

3.139 For the reasons set out below, we have decided to not make any changes to our Guidance in light of stakeholder feedback to our consultation.

3.140 While we recognise the desire for greater certainty about the circumstances in which we might require the use of accredited technology on content communicated privately, we are not persuaded (for the same reasons as set out at paragraph 3.23 above) that it is necessary or appropriate to do so at this stage.

3.141 We also do not consider that our powers are limited to only those parts and functionalities of a service on which there is evidence of relevant content being communicated. We therefore do not consider it appropriate to include such a constraint in our Guidance. However, we would consider evidence of the parts and functionalities where the content is present (including from the skilled person, where relevant) as part of assessing what is necessary and proportionate. Further, as is made clear in paragraph 3.13(a) of the Guidance, we might only require the use of technology on parts of a service, or in respect of certain functionalities.

3.142 We understand the concern raised by one stakeholder about the risk of a Technology Notice placing disproportionate and duplicative burdens on a provider if it includes requirements about its complaints procedures. As the stakeholder notes, sections 21 and 32 of the Act already require all providers of Part 3 services to operate a complaints

[104] [✂] response to December 2024 Consultation, p.17.
[105] [✂] response to December 2024 Consultation, p.5.
[106] [✂] response to December 2024 Consultation, p.5.

procedure and our Codes of Practice set out recommendations about how providers may do so in a manner consistent with the Act. Where we are considering including provision in a Technology Notice about a provider's complaints procedures under sections 125(3) or (4) of the Act, we would expect to have regard to the provider's existing complaints procedures and to satisfy ourselves that the imposition of additional requirements is proportionate. We do not however consider it necessary to amend our Guidance in light of this submission and note that paragraph 3.13(c) already makes clear that we would carefully consider the wider systems and processes that we require in a Technology Notice, and that what is necessary and proportionate may vary on a case-by-case basis.

4. Initial assessment

Introduction

4.1 Our Online Safety Enforcement Guidance sets out the typical initial assessment process we will carry out when an issue comes to our attention. In section 4 of our Guidance, we note that a Technology Notice is one of the regulatory tools available to us to resolve an issue. We also explain how section 4 builds upon the Online Safety Enforcement Guidance by explaining what might prompt us to initially consider exercising our Technology Notice functions (including how we might consider our power to issue a Technology Notice as part of the typical initial assessment process when we become aware of an issue that relates to terrorism and/or CSEA content), and the potential outcomes of an initial assessment.

4.2 Having carefully considered the responses from stakeholders, we have amended paragraph 4.12 of the Guidance.

Overview of stakeholder responses

4.3 Stakeholders commented on three main areas of section A4 of the draft guidance:

a) how issues may come to Ofcom's attention;

b) consideration of the Specified Matters at the initial assessment stage; and

c) engagement with service providers.

4.4 We address each thematic area in turn below.

How issues may come to Ofcom's attention

Summary of draft guidance

4.5 In paragraphs A4.3 and A4.4 of our draft guidance, we explained that we expect the sources of information that might lead us to consider exercising our Technology Notice functions are likely to be the same as those we use to identify and assess potential compliance issues, as set out in our Online Safety Enforcement Guidance. We also provided some examples of what these sources include, such as an issue coming to light through our regular engagement with a service provider or industry, routine monitoring of information provided to Ofcom, and information provided to us by other bodies.

4.6 The draft guidance also explained that we would not be likely to consider exercising our Technology Notice functions based on a complaint of a single piece of relevant content being present on a service, noting that the online safety regime is about service providers' safety systems and processes rather than regulating individual pieces of content found on such services. However, we also went on to state that if we were to receive several complaints which indicate that relevant content may be prevalent on or disseminated by means of a service this would be relevant to our assessment of whether it may be appropriate to exercise our Technology Notice functions.

Summary of stakeholder responses

4.7 The Marie Collins Foundation strongly encouraged Ofcom to reconsider our position that a single piece of relevant content being present on a service would be unlikely to trigger consideration of exercising our Technology Notice functions.[107] They stated that "[a]ny CSEA content represents actual abuse of a child/children" and that, where a complaint is made, we should take immediate action. They suggested that the presence of any CSAM on a service is evidence the providers' systems and processes "are not robust enough".

4.8 Another stakeholder sought clarity on the volumes "several" complaints will amount to in different risk scenarios, and in particular confirmation that this cannot be a low number of total complaints or relate to numerous occurrences of the same piece or type of content.[108]

4.9 The NSPCC expressed concern that relying on provider reported instances of CSEA alone would "mean missing many cases" and encouraged Ofcom to use a wider range of inputs, including regular engagement with civil society organisations and "participation work" with children.[109]

Our response

4.10 We have carefully considered the views submitted and have decided not to make any amendments to the Guidance. We are satisfied that the drafting, at paragraphs 4.3 and 4.4 of the Guidance, reflects the breadth of information sources, the statutory framework and the need to assess matters on a case-by-case basis.

4.11 We acknowledge that any instance of CSEA represents serious harm. However, the Online Safety regime is about service providers' safety systems and processes, not about regulating individual pieces of content found on such services. A single piece of content, on its own, may not necessarily mean that the service provider is failing to fulfil its duties under the Act. As explained in paragraph 3.5 of the Guidance, when deciding whether it is necessary and proportionate to issue a Technology Notice we must consider the Specified Matters including the "prevalence" of relevant content on the service (or of search content of the service that is relevant content (as applicable)). For these reasons, we do not consider it appropriate to amend the Guidance to state that a single piece of relevant content will always lead to an initial assessment.

4.12 We have considered the request from a stakeholder for greater clarity about the reference to "several complaints" in paragraph 4.4 of the Guidance. However, prescribing a numerical or fixed threshold would not be appropriate and would be inconsistent with our more general approach in the Online Safety Enforcement Guidance. The number of complaints that may be relevant to our assessment will depend on, for example, the time period over which the complaints are made, the nature of the service, the quality and consistency of the information provided and the context in which the complaints arise. A rigid definition could lead to outcomes that are either disproportionate or insufficiently responsive to individual circumstances. We therefore consider that the wording in the Guidance sets out a suitable and proportionate approach.

---

[107] Marie Collins Foundation response to December 2024 Consultation, pp.5-6.
[108] [✂] response to December 2024 Consultation, p.18.
[109] NSPCC response to December 2024 Consultation, pp.6-7.

4.13 We recognise the concern that provider reported CSEA content may not reflect the full extent of harm. Ofcom routinely draws on multiple sources of evidence, including organisations working directly with children. This enables Ofcom to consider information that may not otherwise be available to providers and ensures assessments are based on a range of relevant evidence. The examples of sources of information set out in paragraph 4.3 of the Guidance are not exhaustive. Paragraph 3.5 of the Online Safety Enforcement Guidance also sets out further examples of the sources of information Ofcom may use to identify and assess potential compliance issues. For these reasons, we do not consider the Guidance needs to be amended to reflect the range of inputs Ofcom will consider.

Consideration of the Specified Matters at initial assessment stage

Summary of draft guidance

4.14 Paragraph A4.8 of the draft guidance explained that where Ofcom is considering whether it would be appropriate to exercise our powers to issue a Technology Notice as part of our initial assessment, we would expect to take into account, to the extent we are able to, the Specified Matters in assessing whether it may be necessary and proportionate to issue a Technology Notice.

Stakeholder response

4.15 A stakeholder raised concerns that a detailed consideration of the Specified Matters would not commence until the Warning Notice stage, posing a risk to users' human rights. They sought assurance that the Specified Matters, particularly those relating to human rights, are always given due weight at the initial assessment stage, particularly where this results in Ofcom concluding that a Technology Notice may be appropriate.[110]

Our response

4.16 We consider that the existing drafting at paragraph 4.8 of the Guidance appropriately reflects the preliminary nature of initial assessments, while ensuring the Specified Matters, including human rights considerations, are taken into account at this stage to the extent that is possible.

4.17 The Act does not specify a legal test that Ofcom should apply when considering whether it may be appropriate to exercise our powers to issue a Technology Notice as part of our initial assessment. We explain in the Guidance that we would expect to take into account, to the extent that we are able to, the Specified Matters. As set out in section 3 of the Guidance, the Specified Matters, including those relating to users' rights to freedom of expression and privacy, form only one part of Ofcom's overall assessment of whether issuing a Technology Notice would be necessary and proportionate.

4.18 Paragraph 4.8 of the Guidance reflects that an initial assessment is a preliminary and proportionate process, undertaken on the basis of the information available at that stage. The initial assessment is the first step in the process, and it is not until we are considering whether to issue a Warning Notice that we will be in a position to make a more detailed

[110] [✂] response to December 2024 Consultation, p.18.

assessment of the Specified Matters. This will of course include a proper assessment of human rights impacts, when we have the relevant information necessary to make such an assessment.

Engagement with service providers

Summary of draft guidance

4.19 Paragraph A4.9 of the draft guidance explained that as part of our initial assessment, Ofcom may engage with the service provider to give them an opportunity to comment on the issue(s), and to provide information to assist us in determining what action, if any, we should take.

Summary of stakeholder responses

4.20 Several stakeholders suggested that Ofcom should always engage with service providers during an initial assessment.[111] Reasons given in support of this included that:

a) engaging with service providers during an initial assessment would help Ofcom better understand a provider's existing content moderation tools (which is important to understand the need for a Technology Notice and inform any next steps) and give providers the opportunity to best respond to our concerns; [112]

b) the provider's assistance will likely be required to verify the source of any complaints;[113] and

c) a commitment to engaging with providers at this stage ensures consistency and fairness.[114]

Our response

4.21 The position that we have taken in our Guidance is in line with the approach to initial assessments set out in our Online Safety Enforcement Guidance. We are not persuaded that there is a need to depart from this approach. We remain satisfied that the Guidance accurately reflects the flexibility required to discharge our statutory functions effectively. This wording ensures that engagement takes place where it would meaningfully support the initial assessment, while preserving the discretion necessary to act proportionately, promptly and with due regard to complainant sensitivity.

4.22 Paragraph 4.9 of the Guidance should be read alongside paragraphs 4.8 to 4.14 of Ofcom's Online Safety Enforcement Guidance, which sets out our usual process for how we will engage with service providers during an initial assessment. This explains that, where we are carrying out an initial assessment following receipt of a complaint from an industry stakeholder, other enforcement agency or whistleblower, we will generally tell the service provider and share a non-confidential version of the complaint with them for comment.[115]

---

[111] [✂] response to December 2024 Consultation, p.6; Google response to December 2024 Consultation, p.15; [✂] response to December 2024 Consultation, pp.17-18; [✂] response to December 2024 Consultation, p.2.
[112] Google response to December 2024 Consultation, p.15; [✂] response to December 2024 Consultation, pp.17-18.
[113] [✂] response to December 2024 Consultation, pp.17-18.
[114] [✂] response to December 2024 Consultation, p.6.
[115] Online Safety Enforcement Guidance, See Section 4, paragraph 4.9.

It also includes examples of the circumstances in which we may decide not to engage with a service provider during an initial assessment, such as where we consider that we already have sufficient information to conduct our initial assessment and decide the appropriate next steps, where there are reasons to take action more quickly, or where it is important to safeguard the anonymity of a complainant.

4.23 It is important to note that the purpose of the initial assessment is to decide what action, if any, it may be appropriate to take to resolve the issue. We have a variety of tools we can use to resolve an issue and at this stage we are only considering whether it may be necessary and proportionate to issue a Notice. As explained in paragraph 4.13 of the Guidance, starting the initial assessment process does not imply that we are satisfied that it would be necessary and proportionate to issue a Notice, nor that we will ultimately do so.

4.24 We do not consider that mandatory engagement is necessarily always needed to ensure Ofcom properly understands a provider's existing technical measures or alternative regulatory routes. Where information would materially assist our initial assessment, we will seek it through engagement with the service provider. This may include using our statutory information gathering powers.

4.25 We do not accept the view that consistency and fairness requires Ofcom to engage with providers during every initial assessment. Our Guidance is intended to be flexible to allow us to consider on a case-by-case basis whether it is appropriate to engage with the service provider. A mandatory requirement to engage could delay action in urgent cases involving serious harm, may require Ofcom to request information that is unnecessary or duplicative, or risk undermining the confidentiality of sensitive information. Such an approach would not align with Ofcom's duties to act proportionately, nor with the principles of being targeted and evidence-based in our regulatory activity.

4.26 If we do decide not to engage with a service provider during an initial assessment, we have amended the Guidance to confirm that, where we consider that it may be necessary and proportionate to issue a Technology Notice, we will inform them of the outcome of the initial assessment (see paragraphs 4.12 and 5.2 to 5.4 of the Guidance) and engage with them during the process (see paragraphs 5.5 to 5.7 of the Guidance).

5. Next steps and approach to information gathering

Introduction

5.1 This section addresses section 5 of the Guidance, which explains the next steps where we consider (following an initial assessment) that it may be necessary and proportionate to issue a Technology Notice. The Guidance describes how we will notify and engage with Part 3 providers, our general approach to information gathering (including the use of our statutory information gathering powers), the process for obtaining a skilled person's report, and the duties imposed on providers during this stage.

5.2 Having carefully considered the responses from stakeholders we have amended the Guidance in paragraphs 5.2, 5.5, 5.12, 5.14 and 5.16. These amendments have been made to clarify respectively when Ofcom will engage with the service provider, when the service provider can make representations on the appointment of the skilled person, the assistance that should be provided to the skilled person and the enforcement action that may be taken in respect of Information Notice breaches. Further details of the amendments are explained below.

Overview of stakeholder responses

5.3 Stakeholders commented on four main areas of this section:

a) notification and engagement process;

b) use of information gathering powers;

c) skilled person appointment, independence and payment; and

d) scope of assistance and testing.

5.4 We address each of these areas below.

Notification and engagement process

Summary of draft guidance

5.5 Paragraphs A5.2 to A5.7 of the draft guidance described how Ofcom will engage with a provider if we consider that issuing a Technology Notice may be necessary and proportionate. It explained that we would typically notify the provider of our decision via email, setting out the project team, a summary of our concerns, next steps and likely timescales, and information on how to complain.

5.6 The draft guidance also stated that we expect to engage with the provider during the process, for example before obtaining a skilled person's report or using any of our other information gathering powers. It explained that we will generally provide updates to the provider on our progress, including when we expect to reach certain milestones, and may meet with the provider where we consider it appropriate for reasons of fairness and transparency.

Stakeholder response

5.7 One stakeholder suggested that, given the importance of early and ongoing dialogue with affected providers, Ofcom should consider amending paragraph A5.5 of the draft guidance to say it "will" engage with the service provider.[116] X made a similar (albeit more general) comment that providers should be involved in the decision-making process, suggesting that this is not currently clear.[117]

Our response

5.8 We have amended paragraph 5.2 of the Guidance to confirm that we will inform the service provider of the outcome of the initial assessment where we consider it may be necessary and proportionate to issue a Technology Notice. We have also updated paragraph 5.5 of the Guidance to state that we "will" engage with the service provider during the process where we consider (following an initial assessment) that it may be necessary and proportionate to issue a Technology Notice.

Use of information gathering powers

Summary of draft guidance

5.9 Paragraphs A5.8 to A5.10 of the draft guidance set out our approach to information gathering during this stage. It explained that, while we must obtain a skilled person's report before issuing a Technology Notice, we may also use our other information gathering powers under the Act (either before obtaining a skilled person's report or concurrently). This could, for example, assist in determining what skilled person(s) to appoint or what issues they should address; obtaining information for compatibility testing; or confirming that information provided by the service provider during the initial assessment stage is accurate and complete. Where we use our information gathering powers, our draft guidance noted that we will do so in line with our Online Safety Information Powers Guidance.

5.10 Paragraph A5.10 noted that where appropriate, we may also gather information from sources using other methods, such as from public sources, through informal or voluntary engagement with services, or from other bodies (e.g. other regulators or law enforcement agencies).

Summary of stakeholder responses

5.11 The NSPCC stated Ofcom's information gathering powers will be important for informing compatibility testing and validating information obtained in the initial assessment stage. They also stated that it is important that Ofcom's information gathering powers are not only used in the context of issuing Technology Notices, but also to fully understand the technology landscape such as the applicability of technologies in different settings and whether possible technologies could be in the pipeline for accreditation.[118]

[116] [✂] response to December 2024 Consultation, p.19.
[117] X response to December 2024 Consultation, p.6.
[118] NSPCC response to December 2024 Consultation, p.4.

5.12 In addition, the NSPCC strongly supported Ofcom's strong enforcement powers, including senior manager liability and financial penalties for platforms that fail to comply, and suggested these should be laid out in the guidance.

5.13 The NSPCC also stated that the skilled person's report will be useful in determining how technology may be applied if a Notice is issued.[119]

5.14 One stakeholder sought clarity on the statement in paragraph A5.10 that "we may also gather further information from sources using methods other than our information powers". They requested clarity on the practical scenarios when this additional information may be requested or obtained.[120]

Our response

5.15 We have considered the comments from stakeholders and, except as set out at paragraph 5.18 below, we do not consider that amendments need to be made to the Guidance.

5.16 We recognise the value of using our information gathering powers to develop our understanding of the technology landscape, including technologies that may be available or in development. Our information gathering powers may be exercised for a range of purposes under the Act, including understanding compliance with duties and assessing risks more broadly. However, section 5 of the Guidance specifically addresses information gathering at the stage where we are considering whether to issue a Technology Notice in a particular case. At this stage, and for the avoidance of doubt, the purpose of information gathering is to inform our consideration of whether to issue a Technology Notice in the specific case under consideration.

5.17 The principles set out in section 4 of the Online Safety Information Powers Guidance including data protection, confidentiality and proportionality considerations, apply when we exercise our information gathering powers at this stage. The Guidance cross-refers to the Online Safety Information Powers Guidance, which sets out these considerations in detail and we will exercise our powers in accordance with those principles.

5.18 We have however amended paragraph 5.16 of the Guidance to also refer to the criminal offences which are associated with non-compliance with Ofcom's information powers, and that these may apply not only to the service provider but also, for example, to a named senior manager.

5.19 Paragraph 5.10 of the Guidance notes that we may, where appropriate, gather information using methods other than our statutory information gathering powers. Examples include publicly available information on services' websites, information provided voluntarily by services in response to informal requests, or information shared by other bodies such as regulators or law enforcement agencies. The circumstances in which we might use such methods will vary but would typically be where such information is relevant to our consideration and can be obtained efficiently without the need to exercise our statutory powers.

[119] NSPCC response to December 2024 Consultation, p.4.
[120] [✂] response to December 2024 Consultation, p.19.

Skilled person appointment, independence and payment

Summary of draft guidance

5.20 Paragraphs A5.11 to A5.13 of the draft guidance set out our approach to obtaining skilled person's reports. They explained that the purpose of such a report is to assist Ofcom in deciding whether to issue a Technology Notice and to advise about the requirements that might be imposed. Where we obtain a skilled person's report for Technology Notice purposes, our draft guidance noted that we will have regard to section 5 of our Online Safety Information Powers Guidance.

5.21 Our draft guidance also noted that:

a) the skilled person must be appointed by Ofcom;

b) we will typically notify the service provider of the appointment via email and specify the relevant matters to be explored in the report; and

c) the provider is liable for payment of the skilled person's remuneration and expenses.

5.22 The draft guidance explained that the relevant matters we will ask a skilled person to advise on will depend on the specific circumstances and may, for example, include explaining the provider's existing systems and processes to identify relevant content, and how (and where) accredited technology could be implemented alongside this, or providing information on the prevalence of such content on the service. Our draft guidance noted that we may also request the skilled person conduct separate testing or suggest testing that Ofcom may undertake.

Summary of stakeholder responses

5.23 The NSPCC welcomed that the skilled person must be appointed by Ofcom rather than the service, stating this is important in ensuring both independence in the process and robustness in gathering appropriate information.[121]

5.24 However, a number of respondents emphasised the importance of providers having a role in the appointment process. For example, a stakeholder sought clarity that Ofcom would ask for a provider's nominations, recommendations or objections regarding the identity of the skilled person where appropriate.[122] Similarly, X requested confirmation that they will be able to nominate a skilled person,[123] and Google explained that it is critical that service providers have the opportunity to review and raise objections about the appointment of the skilled person on grounds of conflict of interest, confidentiality or security issues.[124]

5.25 One stakeholder emphasised the importance of independence and sought clarity from Ofcom on ensuring the independence of a skilled person, noting that skilled persons may access providers' systems.[125]

[121] NSPCC response to December 2024 Consultation, p.5.
[122] [✂] response to December 2024 Consultation, p.19.
[123] X response to December 2024 Consultation, p.2 and p.6.
[124] Google response to December 2024 Consultation, pp.16-17.
[125] [✂] response to December 2024 Consultation, p.20.

5.26 Another stakeholder suggested that the draft guidance does not contain sufficient information about how Ofcom will judge the evidence of actual harm, specifically the prevalence of relevant content on the service and the extent of dissemination. They stated that Ofcom should commit to always asking the skilled person to assess the scale, extent and nature of any harm and to ask the skilled person to advise on whether an intervention would be necessary and proportionate.[126]

5.27 Google commented that any payment arrangement for a skilled person should be time bound and governed by a set fee arrangement, or service providers should be allowed to object to fees outside a certain range where not proportionate.[127]

5.28 Another stakeholder noted that the focus of a skilled person's report will be deeply technical, and the importance of independence means there is a real chance that the draft report will contain misapprehensions about the nature of a service's existing controls. They suggested that issuing the report in draft would allow any such defects to be reviewed promptly and would allow Ofcom to avoid progressing its escalation of the process in cases where complex services or existing controls have been misunderstood.[128]

Our response

5.29 As discussed above, comments relating to the use of skilled persons tended to focus on: (a) the role of providers in the appointment of a skilled person, (b) the need for a skilled person to be independent and maintain confidentiality, (c) the scope of the skilled person's reports, (d) payment for skilled persons, and (e) the need for providers to review skilled person's reports at draft stage. We summarise stakeholders' responses on each of these in turn below.

Appointment process and provider contribution

5.30 The requirement for Ofcom to appoint skilled persons in relation to Technology Notices is a statutory requirement under section 122(1) of the Act.

5.31 Having carefully considered the comments from stakeholders we have amended the Guidance, at paragraph 5.12, to confirm that we will give the service provider the opportunity to provide representations on whether a specific skilled person may, or may not be, suitable before Ofcom decides which skilled person will be appointed.

Independence and confidentiality safeguards

5.32 Paragraph 5.5 of the Online Safety Information Powers Guidance already addresses concerns about independence and conflicts of interest. In particular, it makes clear that we are only likely to consider that a person has the skills necessary to prepare a report about relevant matters where that person is independent from the service or service provider or can otherwise demonstrate no conflict of interest could arise.[129] It also explains that Ofcom is only likely to appoint a skilled person where we are satisfied that the person has appropriate safeguards in place to ensure confidential information is not disclosed to anyone other than Ofcom.[130] This will be considered on a case-by-case basis. As noted

[126] [✂] response to December 2024 Consultation, p.6.
[127] Google response to December 2024 Consultation, p.17.
[128] [✂] response to December 2024 Consultation, p.20.
[129] See section 5 of Online Safety Information Powers Guidance.
[130] Online Safety Information Powers Guidance

above, the service provider will also have the opportunity to raise any concerns in its representations before we decide which skilled person to appoint.

5.33 Further, information provided to a skilled person, and the content of their report, will be subject to the general prohibition on disclosure set out in section 393 of the Communications Act.[131]

Harm prevalence assessment and scope of skilled person's role

5.34 Paragraph 5.13 of the Guidance explicitly states, by way of example, that we might ask a skilled person to provide information on the prevalence of terrorism or CSEA content (as the case may be) on the service. This is in recognition of the fact that the scale and nature of harm on a service will be an important consideration in our assessment of whether issuing a Technology Notice is necessary and proportionate. However, the Guidance also makes clear that the specific matters we ask a skilled person to address will depend on the specific circumstances and issue we are considering, including what information is already available to us.

5.35 Having considered stakeholders' comments on the scope of the skilled person's report, we do not believe that it is necessary to amend the Guidance. In particular, we do not consider that it will always be necessary for the skilled person to provide information about the prevalence of relevant content on the service. We may already have sufficient information about harm prevalence from other sources, such as transparency reports, information gathered under our information gathering powers or data from other bodies (for example, other regulatory bodies, civil society organisations or enforcement agencies). Further, and consistent with paragraphs 5.15 to 5.19 above, we are mindful of the need for the exercise of our information gathering powers (including the use of skilled person's reports) to be proportionate.

5.36 We also do not consider that it would be appropriate (or is indeed necessary) for the skilled person to provide a view on whether it is necessary and proportionate to issue a Technology Notice in a particular case. This will ultimately be a matter for Ofcom, taking into account all relevant evidence and in accordance with our statutory duties. The skilled person's role is to provide technical expertise to assist Ofcom's decision-making and to advise about the requirements that might be imposed by a Notice (if it were to be given), rather than to determine questions of necessity and proportionality.

Payment and fee arrangements

5.37 We do not consider it appropriate to commit to specific fee structures in the Guidance. The commercial arrangements for a skilled person's costs will need to be considered on a case-by-case basis, taking into account the complexity and scope of the particular Technology Notice under consideration. Some skilled persons may or may not accept set fee arrangements and committing to such arrangements in our Guidance could limit our ability to appoint appropriately qualified skilled persons with the necessary expertise. It is important that the Guidance provides Ofcom with flexibility to ensure we can secure the most suitable skilled person for each case.

5.38 Paragraph 5.6 of the Online Safety Information Powers Guidance confirms we will exercise our power to appoint a skilled person in a proportionate manner and section 3 of that

[131] Section 393 of the Communications Act (general restrictions on disclosure of information), see section 115 of the Act, Part 4, Chapter 4.

guidance sets out the factors we will generally take into account when making this assessment, including the cost or impact to the person who would be subject to the power (such as the cost of appointing a skilled person).[132]

Timing of sharing skilled person's reports

5.39 We have amended the Guidance, at paragraph 6.6, to confirm that the service provider will be provided with copies of, or access to, the skilled person's report (in final form) alongside the Warning Notice (redacted where appropriate). We do not consider it appropriate to share a summary or copy of the draft report. At the Warning Notice stage, providers will have the opportunity to make representations on the content of the report and on our intention to issue a Technology Notice. This is consistent with the approach that we have taken in the Online Safety Information Powers Guidance. Furthermore, we consider the risk of the report containing misunderstandings is low given the duty to give all such assistance to the skilled person as they may reasonably require (discussed at paragraphs 5.46 to 5.47 below below).

5.40 We have also noted in the Guidance (at footnote 75) that rather than providing copies of documents we rely on which Ofcom has already disclosed to the service provider, or were provided to us by the provider, with the Warning Notice we may instead list these in a schedule for the service provider to cross-refer to their own copies.

Scope of assistance and testing

Summary of draft guidance

5.41 Paragraph A5.13 noted that we may request that a skilled person conduct separate testing or suggests any testing that Ofcom may undertake when we are considering whether to issue a Technology Notice.

5.42 Paragraphs A5.14 and A5.15 of the draft guidance explained the duties placed on service providers when Ofcom exercises its information gathering powers (including to give the skilled person all such assistance as they may reasonably require in preparing the report) and the potential consequences of non-compliance.

Summary of stakeholder responses

5.43 The NSPCC and Marie Collins Foundation welcomed the recognition in the draft guidance that providers are required to give all such assistance as the skilled person may reasonably require,[133] with the NSPCC also welcoming the reiteration that failure to comply may lead to significant consequences, including the imposition of a financial penalty.[134]

5.44 However, Google explained that it would appreciate further clarity on the scope of assistance to be provided to skilled persons. It expressed concern that the requirement to provide all such assistance as may be reasonably required effectively provided a skilled person with an unbounded audit right over Google's technologies.[135] While it (and another

[132] See section 3 of the Online Safety Information Powers Guidance which sets out in greater detail Ofcom's general approach to online safety information gathering.
[133] NSPCC response to December 2024 Consultation, p.5; Marie Collins Foundation response to December 2024 Consultation, p.5.
[134] NSPCC response to December 2024 Consultation, p.5.
[135] Google response to December 2024 Consultation, pp.17-18

stakeholder) welcomed the clarification in the Online Safety Information Powers Guidance that this duty does not extend to legally privileged material,[136] Google noted that it would appreciate additional limitations, guardrails or explanations on what assistance is required, including clarification on how a provider may raise objections if they believe certain assistance is not reasonably required.[137]

5.45 Google also asked for clarification about the scope of any additional testing conducted by a skilled person and how it would occur.[138] It noted some of the challenges associated with independent testing (such as difficulties in dataset collection) and requested that Ofcom explicitly reference the considerations listed in section 4 of the Online Safety Information Powers Guidance (in particular, the data protection considerations in paragraph 4.64).[139]

Our response

Duty to assist

5.46 The duty set out in section 104(7) of the Act requires a service provider, and anyone who works for the service (or used to work for the service), or who is providing services to the service provider on relevant matters, to give the skilled person all such assistance as they may reasonably require to prepare the report. This is a statutory requirement, reflecting the importance of skilled persons being able to obtain information necessary to provide Ofcom with informed advice. We have updated paragraph 5.14 of the Guidance to reflect that the duty to provide assistance to the skilled person does not fall only on the service provider – in line with the wording of the Act.

5.47 The statutory duty to provide assistance is expressly limited by the requirement of reasonableness. In particular, it does not extend beyond what is 'reasonably' required by the skilled person to prepare its report. This is clear on the face of the Act, and we do not consider that it is necessary to revise our Guidance in order to provide further clarification on this. We note that what will be reasonably required by a skilled person will likely depend on a case-by-case basis. Notwithstanding this, we have decided to align our Guidance with paragraphs 3.19 and 5.17 of the Online Safety Information Powers Guidance. In particular, by recognising explicitly in our Guidance (see paragraphs 5.14 and 5.15) that:

a) we do not consider that the duty to provide assistance to a skilled person requires those subject to it to provide information subject to legal professional privilege; and
b) where providers have concerns about the proportionality of assistance requested, they may raise this in writing with the responsible Ofcom Director.[140] This allows the provider to explain why they consider particular requests may not be reasonably required in the circumstances.

Testing authority and data protection

5.48 The reference in paragraph 5.13 of the Guidance to Ofcom potentially requesting that a skilled person conduct separate testing is permissive rather than presumptive. Whether such testing is appropriate and the scope of any such testing will depend on the specific

[136] [✂] response to December 2024 Consultation, p.20.
[137] Google response to December 2024 Consultation, p.17.
[138] Google response to December 2024 Consultation, pp.17-18.
[139] Google response to December 2024 Consultation, pp.17-18.
[140] We will confirm who the responsible Ofcom Director is when we notify the service provider of the outcome of our initial assessment.

circumstances, including what information is already available to Ofcom and what is needed to inform our decision-making. We are not persuaded that it is necessary for our Guidance to provide further detail on this at this stage.

5.49 We are also not persuaded that it is necessary for our Guidance to provide detail on how such testing might occur at this stage. The testing required will be specific to the service provider and will be considered on a case-by-case basis.

5.50 Where testing is considered necessary, this would of course be undertaken with regard to section 4 of the Online Safety Information Powers Guidance, including compliance with data protection legislation, the need to protect confidential information, and the proportionality of information gathering activities.

6. Deciding whether to issue a Technology Notice

Introduction

6.1 Section 6 of the Guidance explains the stages of our process from deciding whether to issue a Warning Notice, through to making the final decision on whether to issue a Technology Notice. This includes the information that will be contained in a Warning Notice; the opportunity for service providers to make representations; and the information that would be contained in a Technology Notice if one were issued.

6.2 We have decided to amend paragraph 6.6 of the Guidance to confirm that the skilled person's report (in final form) will be provided to service providers alongside any Warning Notice, and paragraph 6.5(b) to make clearer that Ofcom will not require providers to make technology they have developed or sourced pursuant to a Technology Notice available for use by other service providers in a Notice to use accredited technology.

Overview of stakeholder responses

6.3 Stakeholders commented on the following areas of this section of the draft guidance:

a) Content and transparency of Warning Notices;

b) The Warning Notice process;

c) Timeframe for representations; and

d) Timescales for compliance and the duration of a Technology Notice.

Content and transparency of Warning Notices

Summary of draft guidance

6.4 Paragraph A6.5 of the draft guidance set out the information that will be contained in a Warning Notice. This includes the reasons why Ofcom provisionally considers it necessary and proportionate to issue a Technology Notice, and a summary of the skilled person's report together with any other evidence on which we have relied to reach our provisional conclusions. The draft guidance also noted that the Warning Notice will set out the requirements we are considering imposing, for what period, and the timescales for compliance and/or steps to be taken.

Summary of stakeholder responses

6.5 Google suggested that, in order to make fulsome representations, the entire skilled person's report and related information should be made available to the service provider rather than a summary including, for example, information disclosed to the skilled person

to prepare the report, the specific requests that Ofcom asked to be included in the report or any evidence relied on by the skilled person.[141]

6.6 Drs Shurson, Keenan and Ó Floinn commented that the draft guidance lacked sufficient detail on the practical consequences of a Notice to develop or source technology. For example, they noted that, at paragraph A6.5(b), it states that we would not require a service provider to allow technology they have developed or sourced to be used by another service provider in a Notice but this is not categorically ruled out and there is no discussion of the intellectual property implications.[142]

Our response

6.7 We recognise that service providers require sufficient information to make meaningful representations. As discussed at paragraphs 5.39 to 5.40 above, we have therefore amended paragraph 6.6 of the Guidance to confirm that, alongside the Warning Notice, we will provide a copy of (or access to) the skilled person's report (in final form), together with the key evidence and information relied upon by the skilled person in preparing their report, and any other evidence or information we have relied upon in reaching our provisional conclusions. Paragraph 6.5(a) remains unchanged as, in line with sections 123(2)(a) and 123(3)(a) of the Act, the Warning Notice itself will still include a summary of the skilled person's report.

6.8 Amongst other things, paragraph 6.5(b) of the Guidance seeks to make clear that if a provider develops technology pursuant to a Notice to develop or source technology, which ultimately meets the minimum standards of accuracy, Ofcom will not then require that provider to make that technology available for use by another provider in a Notice to use accredited technology (while we would equally not prevent providers licensing it for use by other providers). We have modified the wording in our Guidance to better reflect this.

Warning Notice process

Summary of draft guidance

6.9 Paragraphs A6.2 to A6.10 of the draft guidance provided detail on Ofcom's decision to issue a Warning Notice. Amongst other things, it explained that Ofcom would issue a Warning Notice to the relevant provider if (having considered the skilled person's report and any other relevant evidence) we provisionally consider that it is necessary and proportionate to issue a Technology Notice. It noted that we will not issue a final Technology Notice until after the period for the provider to make representations has passed.

Summary of stakeholder responses

6.10 The Marie Collins Foundation said they are not convinced by the need to issue a Warning Notice. They are concerned that they offer providers advance notice and might lead to concealment or diversion issues and allow providers too much latitude to effectively appeal or rebuff a potential Technology Notice. They suggested that it would be preferable for

[141] Google response to December 2024 Consultation, p.18.
[142] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.3.

Ofcom to allow for engagement with service providers after the Technology Notice has been issued.[143]

Our response

6.11 The Guidance reflects the statutory framework established by Parliament. The requirement to issue a Warning Notice is set out in section 123 of the Act. Section 123(1) provides that we may only issue a Technology Notice after first issuing a Warning Notice stating that we intend to give such a Notice.

6.12 The Warning Notice process also serves an important purpose. It provides service providers with a meaningful opportunity to make representations on whether a Technology Notice is necessary and proportionate in their specific circumstances, and to supply additional evidence that we may not have previously considered. This helps ensure that any final decision is based on a complete and accurate understanding of the relevant facts.

6.13 We also note that the representations process will not give providers an open-ended opportunity to delay or avoid regulatory action. We will specify the period within which representations must be made and, once that period has expired, we will proceed to a final decision. As explained at paragraph 6.3 of the Guidance, issuing a Warning Notice does not mean a Technology Notice will necessarily follow; that decision will be taken only after we have considered any representations received.

Timeframe for representations

Summary of the draft guidance

6.14 Paragraph A6.8 of the draft guidance stated that Ofcom will typically give a period of at least 20 working days to make written representations in response to the Warning Notice. It acknowledged however that the period will depend on the individual circumstances and that there may be circumstances where service providers require a longer period to provide representations (or, in exceptional circumstances, where an expedited process is appropriate).

Summary of stakeholder responses

6.15 Several respondents expressed concern about providers only having 20 working days to make representations in response to the Warning Notice, most highlighting the potentially complex and technical nature of any response.[144]

6.16 While X sought a longer period for providers to make representations,[145] one stakeholder asked that Ofcom clarify in the guidance that there will be a presumption in favour of an extension where providers can articulate why it is needed.[146]

[143] Marie Collins Foundation response to December 2024 Consultation, pp.4-5.
[144] Open Rights Group response to December 2024 Consultation, p.4; [✂] response to December 2024 Consultation, p.20; [✂] response to December 2024 Consultation, p.7; X response to December 2024 Consultation, p.6.
[145] X response to December 2024 Consultation, p.6.
[146] [✂] response to December 2024 Consultation, p.7.

6.17 Another stakeholder strongly recommended Ofcom acknowledge the difficulty a provider may have in responding to a Warning Notice within 20 working days and suggested that the guidance should specify examples of the individual circumstances Ofcom will consider when permitting a longer time period. They suggested, for example, that providers who have shown a willingness to engage with Ofcom should be permitted more time to explore alternative solutions and/or demonstrate how existing solutions are able to deal with our concerns.[147]

Our response

6.18 We have carefully considered the responses from stakeholders, but we do not consider that the Guidance requires amendment. The minimum period of 20 working days, combined with the flexibility to extend this period where appropriate based on the specific circumstances of each case, provides an appropriate balance between ensuring providers have sufficient time to make meaningful representations and avoiding unnecessary delays in the regulatory process.

Existing flexibility in the Guidance

6.19 We recognise that responding to a Warning Notice may require engagement with complex technical and legal issues and may place significant demands on provider resources, particularly for large or complex services.

6.20 The Guidance already reflects this by stating that the period for representations "will however depend on the individual circumstances" and that "there may be circumstances where service providers may require a longer period to provide representations."[148] This flexibility is important because the appropriate timeframe will vary depending on, for example, the complexity and urgency of the matters raised, the nature and scale of the service, the service provider's technical architecture and internal processes, as well as the resources available to the provider.

Approach to extension requests

6.21 We do not consider it appropriate to establish a presumption in favour of extension requests to the representation period. The appropriate timeframe for representations must be determined on a case-by-case basis and Ofcom would expect to set a timeframe in a particular case that is achievable (and for which there need not necessarily be a presumption in favour of an extension).

6.22 Further, creating such a presumption could, in our view, introduce unnecessary delays and uncertainty in the regulatory process, potentially to the detriment of users who may be at risk of harm from relevant content. The case-by-case approach set out in the Guidance provides appropriate flexibility while ensuring that timeframes are tailored to the genuine needs of each situation.

6.23 We do, however, recognise the importance of ensuring that service providers have adequate time to make meaningful representations. We would encourage service providers to raise any issues as soon as possible. Where a provider can articulate specific reasons why the specified timeframe would be insufficient, for example, to consult with technical teams across different jurisdictions, or to conduct internal analysis of complex systems, we will

[147] [✂] response to December 2024 Consultation, p.20.
[148] Paragraph 6.9 of the Guidance, p.29.

give such requests serious and careful consideration. The Guidance recognises there may be circumstances requiring longer periods, and this flexibility will be applied in practice where justified.

6.24 We do not agree that the Guidance should permit additional time to provide representations on the Warning Notice to service providers that have shown a willingness to engage with Ofcom. As noted above in paragraph 5.8 above we have updated paragraph 5.5 of the Guidance to state that we "will" engage with the service provider where we consider (following an initial assessment) that it may be necessary and proportionate to issue a Technology Notice. We therefore consider that service providers will have sufficient time to engage with Ofcom before the Warning Notice is issued (for example, to explore alternative solutions and/or demonstrate how existing solutions are able to deal with Ofcom's concerns).

Baseline timeframe and factors

6.25 Having considered stakeholders' responses, we are not persuaded that we should change the reference in our Guidance to providers having at least 20 working days to make representations. This minimum period is intended as a reasonable baseline, consistent with other regulatory contexts, including our Online Safety Enforcement Guidance. As the Guidance makes clear (and other than in exceptional circumstances), this is the *minimum* period for representations that we would expect to provide. As noted at paragraph 6.21 above, the appropriate timeframe for any extension to the 20 working days period to respond will be determined on a case-by-case basis (and as noted above, we will consider requests for an extension where providers can demonstrate that additional time is needed to prepare their response).

Timescales for compliance with Technology Notices and the duration of a Technology Notice

Summary of draft guidance

6.26 Paragraphs A6.18 to A6.20 of the draft guidance explained that any period(s) for compliance that we specify in a Technology Notice will be in line with the Act and assessed on a case-by-case basis, taking account of all relevant information.

6.27 For a Technology Notice requiring the use of accredited technology, the draft guidance noted that we must specify a reasonable period for the service provider to take any action required to comply with the Notice. It also referenced the requirement in the Act that we must specify the period within which the requirements imposed by the Notice will have effect, which may be for up to 36 months (starting from the last day of the compliance period).

6.28 For Notices to develop or source technology, our draft guidance noted that we must specify a reasonable period within which each of the steps specified in the Notice must be taken.

Summary of stakeholder responses

6.29 Two stakeholders commented on the timescales for compliance with a Technology Notice.[149] The NSPCC stated that service providers should be given a maximum period to comply with a Notice, suggesting this should be in line with the periods set out in Ofcom's Codes of Practice. They noted that issuing a Notice means significant harm exists on a platform and they would expect swift compliance to urgently reduce the risk to children.[150] The other stakeholder sought clarity on what constitutes a "reasonable period" and the factors that will be taken into account in assessing this.[151]

6.30 Three stakeholders emphasised the importance of Ofcom giving providers the opportunity to make representations on the period for compliance:

a) Google and another stakeholder explained that incorporating external technologies into a provider's existing processes/systems (or developing or sourcing new technologies) may take significant time,[152] with the other stakeholder adding that the time required will be impacted by factors such as the type of technology, service design and size of the user base.[153] Both stakeholders stressed that providers should have the opportunity to comment on whether any period proposed is feasible;[154] and

b) a further stakeholder suggested that Ofcom should commit to giving providers a further opportunity to make representations on the appropriate compliance period after we have decided to issue a Technology Notice. They argued it was unreasonable to expect providers to have sufficient information to make representations on this issue earlier, as the requirements that Ofcom have decided to impose would not be known until a Notice is issued.[155]

6.31 One stakeholder stated that Ofcom should provide greater detail on the factors that will determine the relevant timeframe for accredited technology to be used, and the opportunity that will be afforded to service providers to make representations about that. In any event, they suggested that this timeframe should be the minimum period necessary to address the relevant content.[156]

Our response

6.32 We recognise the importance of setting achievable compliance timescales that balance the need to swiftly address the harm the Technology Notice is designed to address with the specific characteristics of the service. We consider this can be achieved through the approach outlined in the Guidance.

6.33 As stated in paragraph 6.19 of the Guidance, in determining a reasonable period for compliance, we will assess the circumstances on a case-by-case basis taking into account all relevant information and evidence available and those factors that appear to us to be

[149] NSPCC response to December 2024 Consultation, p.5; [✂] response to December 2024 Consultation, p.20.
[150] NSPCC response to December 2024 Consultation, p.5.
[151] [✂] response to December 2024 Consultation, p.20.
[152] Google response to December 2024 Consultation, p.14; [✂] response to December 2024 Consultation, pp.20-21.
[153] [✂] response to December 2024 Consultation, pp.20-21.
[154] [✂] response to December 2024 Consultation, pp.20-21; Google response to December 2024 Consultation, p.14.
[155] [✂] response to December 2024 Consultation, p.8.
[156] [✂] response to December 2024 Consultation, p.5.

relevant in the circumstances. That could, for example, include consideration of the nature and complexity of the requirements, technical feasibility, the urgency of addressing the underlying concerns and the resources available to the service provider.

6.34 Paragraph 6.5(c) of the Guidance explains that the Warning Notice will set out the period for which we are considering imposing requirements and the proposed timescales for compliance and/or steps to be taken. The Warning Notice process already provides an opportunity for providers to make representations on proposed timescales in paragraphs 6.8 to 6.11 of the Guidance.

6.35 Where a service provider considers that the timescales proposed in a Warning Notice are not realistic, it can raise this in its representations. We will consider such representations in full before deciding what compliance periods to include in any Technology Notice.

6.36 We do not consider it necessary or appropriate to introduce a further, separate opportunity for representations on timescales after a Technology Notice has been issued. The Technology Notice reflects our final decision following the Warning Notice process and consideration of all representations.

7. Next steps after issuing a Technology Notice

Introduction

7.1 Section 7 of the Guidance addresses the steps Ofcom will take following the issuance of a Technology Notice to a service provider, including when we would typically review the service provider's compliance with the Notice and the consequences of non-compliance.

7.2 Having reviewed the comments received from stakeholders we have decided to amend the Guidance, at paragraph 7.3, to clarify that we will engage with the service provider during a review to ensure that we gather all relevant information to assist us in the process. We have also amended paragraphs 7.12 to 7.13 to clarify that providers will have the opportunity to make representations before we issue a further Notice.

Overview of stakeholder responses

7.3 Stakeholders commented on the following areas of Chapter A7 in the draft guidance:

a) Monitoring and reviewing compliance with Technology Notices;

b) Further Technology Notices); and

c) Varying and revoking Technology Notices.

7.4 We address each thematic area below.

Monitoring and reviewing compliance with Technology Notices

Summary of draft guidance

7.5 Paragraphs A7.2 to A7.10 of the draft guidance set out our approach to reviewing compliance with a Technology Notice. They explained that we will generally notify the provider before commencing a review and expect to engage with them during the process.

7.6 For Notices requiring the use of accredited technology, the draft guidance explained that we must carry out a review before the Notice expires and that we would typically expect to begin that review no earlier than six months before that date. For Notices requiring the development or sourcing of technology, it explained that we must review the provider's compliance before the last date by which any step specified in the Notice is required to be taken (such that it is likely that we will conduct a review on more than one occasion).

7.7 The draft guidance noted that the fact the service provider has not been able to develop or source technology which serves the purpose specified by the Notice and meets the minimum accuracy standards of accuracy does not necessarily mean that it has failed to comply with the Notice; we may nevertheless be satisfied that it has used its best endeavours.

Summary of stakeholder responses

7.8 One stakeholder stated the draft guidance should make a much stronger commitment to involve providers in the review process, noting that the guidance provides that Ofcom will only "generally" notify providers before commencing its review of compliance, and that Ofcom "expects", but does not commit, to engage with providers during the review.[157]

7.9 They also stated that the draft guidance does not specify the timing and frequency of reviews and recommended further clarity on the factors that would influence this.[158]

7.10 Two stakeholders also sought further clarification on the meaning of "best endeavours":[159]

a) one stakeholder asked Ofcom to clarify that it may be the case that a provider has satisfied the best endeavours requirement but nevertheless finds that implementing the technology demanded by the Technology Notice is not technically feasible or practicable;[160] and
b) the NCA suggested that the best endeavours definition needs to be clear as they are primarily subjective, which could lead to differing standards across technologies.[161]

Our response

7.11 Having considered stakeholders' responses to our consultation, we have amended paragraph 7.3 of the Guidance to state that we will engage with the service provider during the review to ensure that we gather all relevant information.

7.12 However, we disagree with the assertion that the Guidance does not specify the timing and frequency of reviews and note that paragraphs 7.5 to 7.7 do this. In particular, paragraph 7.5 makes clear that we would typically expect to begin a review of the service provider's compliance with a Technology Notice requiring the use of accredited technology "no earlier than six months before" the date the Notice expires. We also consider in paragraph 7.7 the timing and frequency of reviews in relation to a Notice requiring the development or sourcing of technology. While we recognise that some stakeholders may prefer greater clarity about the steps that might be included in such a Notice, and the periods of compliance with these, this will ultimately depend on the specific facts of the case.

7.13 We also consider that the Guidance at paragraph 7.7 is sufficient to explain that the fact that a provider has not been able to develop or source technology which serves the purpose specified in the Notice and meets the minimum standards of accuracy does not necessarily mean that it has failed to comply, and we may be satisfied that the provider has nevertheless used its best endeavours. Again, this would need to be considered on a case-by-case basis and would include consideration of the evidence provided by the provider.

7.14 We do not therefore consider that there is more that we can say regarding best endeavours (although we may revise our Guidance in the future if we consider it appropriate to do so, including based on our experience in exercising our Technology Notice functions).

---

[157] [✂] response to December 2024 Consultation, p.21.
[158] [✂] response to December 2024 Consultation, p.21.
[159] [✂] response to December 2024 Consultation, p.21; NCA response to December 2024 Consultation, p.4.
[160] [✂] response to December 2024 Consultation, p.21.
[161] NCA response to December 2024 Consultation, p.4.

Further Technology Notices

Summary of the draft guidance

7.15 Paragraphs A7.11 to A7.14 of the draft guidance set out our approach to issuing a further Technology Notice. They explain that we may issue a further Notice if we consider it necessary and proportionate and following consultation with the service provider. Where we decide to issue a further Notice, the draft guidance noted that we are not required to obtain a further skilled person's report or issue a further Warning Notice, but that we may do so where we consider it appropriate to do so (for example, where we are considering imposing substantially different requirements from those contained in the earlier Notice).

Summary of stakeholder responses

7.16 Google said the process for issuing a further Technology Notice should incorporate representations from service providers, suggesting that as drafted the guidance would not require Ofcom to provide service providers the opportunity to make representations and provide evidence of their compliance.[162]

7.17 One stakeholder sought further clarity on the scenarios in which Ofcom may consider it necessary and proportionate to issue a further Notice and the types of "substantially different requirements" that might trigger a further skilled person's report and Warning Notice.[163]

7.18 Drs Shurson, Keenan and Ó Floinn sought further clarity on when a further Technology Notice will be given in relation to any developed or sourced technology and what would be required. For example, they said it is not clear what process would be followed on some points where developed or sourced technology could become subject to a subsequent Notice to use accredited technology (or otherwise), and queried whether safeguards, like the skilled person's report, could be disregarded.[164]

Our response

7.19 We note the stakeholder comments about ensuring service providers have the opportunity to make representations in relation to further Notices. We also recognise that the final sentence of paragraph A7.13 of the draft guidance could be read as suggesting that providers would only have the opportunity to make representations on a further Notice if we decided to issue a Warning Notice.

7.20 For the avoidance of doubt, however, section 126(6) of the Act requires us to consult with the service provider following our review of its compliance and before issuing a further Notice. We have amended paragraphs 7.11 and 7.13 of the Guidance to make clear that this consultation is a statutory requirement and that we will give providers the opportunity to make representations before we issue a further Notice irrespective of whether we issue a Warning Notice or not.

7.21 We note that the Act is not prescriptive about the circumstances in which Ofcom can consider issuing a further Notice, and that whether it is necessary and proportionate to do

[162] Google response to December 2024 Consultation, pp.18-19.
[163] [✂] response to December 2024 Consultation, p.21.
[164] Drs Shurson, Kennan, Ó Floinn response to December 2024 Consultation, pp.3-4.

so will depend on the facts of the case. We do not therefore consider it necessary for the Guidance to provide further detail on the circumstances in which it might be necessary and proportionate to issue a further Notice. These might however include, for example, where a Notice is due to expire but the concerns which led Ofcom to impose the first Notice remain. The Act also makes clear that it may be necessary and proportionate to issue a further Notice in circumstances where we revoke the first Notice (on the basis that we have reasonable concerns about non-compliance with it).

7.22 Whenever we are considering whether it is necessary and proportionate to issue a further Notice (and, if so, what requirements to include in it), we will take into account the matters in section 124 and any other matters we consider to be relevant. This is reflected in paragraph 7.11 of the Guidance.

7.23 Where a review has been conducted in accordance with section 126(4), we would consider the results of that review (including how effective the technology in the first Notice was). The fact that (since the first Notice was issued) terrorism/CSEA content is less prevalent on the service and/or is disseminated less does not necessarily mean that it will not be necessary and proportionate to issue a further Notice. We would expect to consider whether this reduction in prevalence and/or dissemination may reflect, at least in part, the effectiveness of the first Notice.

7.24 What constitutes a "substantially different requirement" (such that we will consider obtaining a further skilled person's report and/or issue a further Warning Notice) will depend on the case. However, examples might include where we are considering requiring the use of a different technology (particularly if it was not considered in the original skilled person's report), or imposing requirements relating to different parts of the service.

7.25 As noted in paragraph 3.118 above, we have amended paragraph 7.13 to note that where we are considering issuing a further Notice requiring the use of technology that has been developed or sourced pursuant to a Notice to develop or source technology, we will issue a further Warning Notice. The assessments at that point will include consideration of the Specified Matters and whether compatibility testing may be appropriate.

Varying and revoking Technology Notices

Summary of draft guidance

7.26 Paragraphs A7.15 to A7.19 set out our approach to varying or revoking Technology Notices. They explained that we may revoke or vary a Notice by notifying the provider to that effect. Revocation might be appropriate, for example, where we have reasonable grounds for believing the provider is failing to comply with the Notice or where we consider the Notice is no longer necessary and proportionate. The draft guidance also noted that variation of a Notice might be appropriate where, for example, new evidence leads us to consider making material changes to it.

7.27 While not required by the Act, paragraph A7.18 of the draft guidance made clear that we will generally engage with service providers before varying or revoking a Notice and will give them an opportunity to make representations on our proposal(s).

Summary of stakeholder responses

7.28 One stakeholder sought clarity on the circumstances in which a provider would be involved in the variation and revocation processes. In particular, they suggested that the draft guidance, at paragraphs A7.17 to A7.18, says that Ofcom will only "notify" providers of a variation though will "generally" allow representations and stated that providers should always have the opportunity to make representations where a Notice is varied to add stricter obligations.[165]

7.29 They further suggested there should be a feedback mechanism or channel for providers to report that an accredited technology is not sufficiently accurate or no longer fit for purpose (for example, because the provider's own technology is more effective) and permitting them to demonstrate their belief using relevant performance data. In addition, they said that providers should be able to request an independent review of the technology or request revocation of the Notice, including revocation pending the conclusion of an expedited assessment where urgent concerns are raised.[166]

7.30 The Open Rights Group said that Ofcom should have a procedure in place for people to raise concerns about any technology deployed that might be exposing users to new cybersecurity risks or infringing on their fundamental rights. [167]

7.31 Two stakeholders also requested clarification on what would happen in the event a technology loses its accreditation. X suggested implementing clear guidelines on whether failing to achieve accreditation standards leads to the revocation of the Notice,[168] while [✂] stressed it was vital that Ofcom defines a process for how we will promptly ensure the revocation of Technology Notices that require use of technology which loses its accreditation.[169]

7.32 Drs Shurson, Keenan and Ó Floinn noted that the Act did not make provision for a service provider to seek review of a Technology Notice prior to initiating an appeal to the Upper Tribunal under section 168 of the Act, and suggested that Ofcom should implement an internal review mechanism to minimise litigation risks and the potential gap in the mechanisms to provide "representations" and "consultations" under, for example, sections 123 and 126 of the Act.[170]

Our response

7.33 We do not consider that it is necessary to amend the Guidance. Paragraphs 7.15 to 7.16 of the Guidance explains that we will consider revoking the Technology Notice where, for example, we have reasonable grounds for believing the service provider is failing to comply, where we consider it is no longer necessary and proportionate for the Notice to remain in effect or where we decide that it is necessary and proportionate to issue a further Notice, taking into account the Specified Matters. As noted in paragraph 7.17 of the Guidance, that includes, for example, where new evidence or information comes to Ofcom's attention such that we would consider making material changes to the Technology Notice. We consider

[165] [✂] response to December 2024 Consultation, p.21.
[166] [✂] response to December 2024 Consultation, pp.13-14.
[167] Open Rights Group response to December 2024 Consultation, p.3.
[168] X response to December 2024 Consultation, p.5.
[169] [✂] response to December 2024 Consultation, p.14.
[170] Drs Shurson, Kennan, Ó Floinn response to December 2024 Consultation, p.9.

the Guidance is sufficient to allow for a review process where there is evidence, including evidence provided by the service provider, public sources (including users) or law enforcement agencies, that the requirements of the Notice are no longer fit for purpose. This would include where information comes to our attention regarding the effectiveness of the technology to achieve the purpose specified in the Technology Notice.

7.34 The Guidance already goes further than the requirements of the Act by stating that we will generally engage with the service provider where we are considering revoking or varying a Technology Notice and will give them an opportunity to provide representations. We consider it appropriate to retain "generally" in paragraph 7.18 of the Guidance to preserve flexibility for circumstances where seeking representations may not be necessary or appropriate. For example, where a provider has requested a specific variation or revocation and we agree to that request.

7.35 However, where we are considering varying a Notice to impose stricter requirements, we would expect to give the service provider the opportunity to make representations.

7.36 We note the suggestion that Ofcom should introduce an internal review mechanism to allow service providers to seek review of a Notice prior to initiating an appeal to the Upper Tribunal. However, we are not persuaded that this is necessary or that it would be appropriate in this case. The Technology Notice process already includes several opportunities for providers to raise concerns *before* a Notice is issued (including before a Notice is varied or a further Notice is issued). Allowing providers to seek internal review of a Notice that has been issued, and which is legally binding, would in our view introduce unnecessary uncertainty (and we note that service providers retain their right of appeal under section 168 of the Act).

8. Disclosure of information and publication

Introduction

8.1 Section 8 of the Guidance outlines our approach to the disclosure of information and publication concerning the exercise of our Technology Notice functions. In particular, it addresses several key matters:

a) the circumstances in which Ofcom may disclose information to third parties, such as a skilled person;

b) our approach to publishing details about decisions to issue Warning Notices and Technology Notices;

c) our obligation to produce an annual report about the exercise of our Technology Notice functions;[171] and

d) the processes by which confidential information will be identified and protected.

8.2 Our Guidance notes that any information that we disclose or publish will be in line with our Online Safety Information Powers Guidance and Online Safety Enforcement Guidance.

8.3 We have considered the points raised by stakeholders and have decided to make one drafting change at paragraph 8.4 of the Guidance to correct an error that was in the draft guidance.

Overview of stakeholder responses

8.4 Stakeholders commented on the following main areas of this section of the draft guidance:

a) transparency and publication of decisions; and

b) confidentiality, security and risk mitigation.

Transparency and publication of decisions

Summary of draft guidance

8.5 Paragraphs A8.4 to A8.11 of the draft guidance set out our approach to publishing details about Technology Notice decisions. It explained that Ofcom is required to have regard to the principle that regulatory activities should be transparent and accountable, and we would expect to publish updates at important milestones, for example, where we issue a Warning Notice or a Technology Notice, or where we issue a further Notice or revoke a Notice.

8.6 The draft guidance stated that where we issue a Warning Notice, we may announce this on our website and, where we do so, would expect to provide details of the service provider, a

[171] The Act requires Ofcom to produce an annual report about the exercise of its Technology Notice functions and technology which meets (or is in the process of development so as to meet) minimum standards of accuracy for the purposes of these functions.

summary of our proposed requirements and a summary of our reasons. Where we issue a Technology Notice or a further Notice, our draft guidance stated that we will generally announce this on our website and provide similar details.

8.7 The draft guidance indicated that while we do not generally expect to publish Technology Notices in full, we will take decisions on a case-by-case basis and may do so in appropriate circumstances. Where we decide to publish a Notice, our draft guidance made clear that we will create a non-confidential version, share it with the service provider prior to publication, and give them the opportunity to provide representations on confidentiality.

8.8 The draft guidance also addressed publication of enforcement actions, business disruption measures, notification procedures to service providers and market sensitive announcements.

Summary of stakeholder responses

8.9 The NSPCC welcomed Ofcom being as transparent as possible in its process, stating that knowing which platforms have been issued with Notices (in relation to CSEA content) will increase understanding of where risks to children exist. They noted this will help researchers, civil society and other platforms understand risk and identify solutions. The NSPCC suggested publishing which specific parts of a platform caused a Technology Notice to be issued to provide clarity, particularly where a service provider owns multiple platforms or where a platform has substantially different parts (such as public and private elements).[172]

8.10 Two stakeholders, raised concerns about paragraph A8.4 of the draft guidance regarding the publication of Warning Notices and suggested that Ofcom should not publicise the issuance of Warning Notices or make public its regulatory intervention until it has decided to issue a Technology Notice .[173] One of those stakeholders added that Ofcom should not make public its regulatory intervention until it has decided to issue a Technology Notice, and suggested that disclosing an intent to issue a Technology Notice in circumstances where Ofcom ultimately accepts a service provider's representations presents a commercial risk to service providers with little upside for regulatory transparency. Their view was that the public interest is in understanding the final outcome of the process rather than the Warning Notice itself.[174] The other stakeholder stated that this approach is not typical of similar regulatory regimes, cited the House of Lords Financial Services Regulation Committee report,[175] and noted that 'naming and shaming' services early in an investigation could undermine the UK's attractiveness as a place to invest and conduct business.[176]

Our response

Publication of Warning Notices

8.11 We recognise that our draft guidance was not as clear as it could have been in relation to the publication of Warning Notices. In particular, while paragraph A8.5 stated that we

[172] NSPCC response to December 2024 Consultation, p.5.
[173] [✂] response to December 2024 Consultation, p.7; [✂] response to December 2024 Consultation, p.22.
[174] [✂] response to December 2024 Consultation, p.7.
[175] Naming and shaming: how not to regulate, House of Lords: Financial Services Regulation Committee, 2025.
[176] [✂] response to December 2024 Consultation, p.22.

"may" announce the issuance of a Warning Notice, paragraph A8.4 suggested that we "would expect" to do so.

8.12 For the avoidance of doubt, the reference to Warning Notices in paragraph A8.4 of our draft guidance was an error, and we have made changes at paragraph 8.4 of the Guidance as a result. Our intention was only to state that Ofcom "may" announce the issuance of a Warning Notice.

8.13 We note the concerns raised by stakeholders about the commercial and reputational implications of publishing Warning Notices, and that – while the NSPCC supported as much transparency as possible in relation to CSEA content – its submission appeared to focus on the benefits of publishing the final Notice. With this in mind, we have removed the reference to Warning Notices in paragraph 8.4 of our Guidance.

8.14 Our view remains, however, that Ofcom should have discretion to publish updates about the issuance of a Warning Notice and that it may be appropriate to do so in some circumstances relating to both terrorism and CSEA content. We note that publication relating to a Warning Notice does not indicate that a decision has been made to issue a final Technology Notice. A final decision will only be reached once our decision-making process has concluded (and after the consideration of representations made by the service provider).

8.15 We consider that the approach in paragraph 8.5 of the Guidance appropriately balances transparency objectives with legitimate concerns about commercial and reputational impacts, and we therefore consider that the Guidance should not be modified. Where we propose to publish information about a Warning Notice, we will have regard to the considerations in paragraph 8.11 regarding market sensitive information and will inform the service provider in advance in accordance with paragraph 8.10.

Level of detail in publications

8.16 When considering how much information to publish about a Notice, we will be mindful of the need to disclose enough information to enable persons with a sufficient interest to exercise their right of appeal under section 168 of the Act (see paragraph 8.6 of the Guidance). This will include disclosing information that identifies the regulated service to which the Technology Notice applies and, where relevant, the specific parts of the service to which the Technology Notice applies.

Confidentiality, security and risk mitigation

Summary of the draft guidance

8.17 Paragraph A8.3 of the draft guidance set out our approach to disclosing information to third parties, including the skilled person.

8.18 Paragraphs A8.4 to A8.11 of the draft guidance explained our approach to publishing details about our decisions. Paragraph A8.10 specifically set out our approach to website updates or media releases.

8.19 Paragraphs A8.16 to A8.18 of the draft guidance addressed our approach to confidential information. They explained that, while we will generally redact or withhold such information, it is occasionally necessary to disclose confidential information to facilitate our regulatory functions. The draft guidance made clear that, if we propose to publish

information which a service provider considers confidential, we will take reasonable steps to inform that service provider and give them a reasonable opportunity to make representations before making a final decision.

Summary of stakeholder responses

8.20 A stakeholder requested clarity on when information will be shared with the skilled person, noting that paragraph A8.3 states this occurs when "relevant" to the purpose of the skilled person's report but that no further safeguards are provided in the guidance regarding privilege or data considerations.[177] They also suggested that Ofcom should clarify that skilled person reports will be treated as containing confidential information about the service provider.[178]

8.21 They also noted that the draft guidance states "blanket" confidentiality requests will not be accepted and requested clarity on whether requests can extend to entire documents or categories of information.[179]

8.22 Another stakeholder raised concerns about paragraph A8.10 of the draft guidance regarding the publication of website updates or media releases about the issuance of a Notice. They stated that Ofcom should commit to providing service providers with an opportunity and a reasonable amount of time to make representations regarding what information the service provider considers to be confidential before any Notice is published (and that Ofcom's justification for providing only one day's notice of such updates or media releases and no opportunity to identify confidential or commercial material is unclear).[180]

Our response

8.23 Having carefully considered stakeholders' responses, our view is that the Guidance remains appropriate. The statutory restrictions in section 393 of the Communications Act, the procedural safeguards in paragraphs 8.16 to 8.18 of the Guidance for parties to make representations on confidentiality, 'the relevance' consideration for disclosure to the skilled person(s), and the requirement for reasoned confidentiality claims together provide appropriate protection for sensitive information while enabling Ofcom to fulfil its transparency and regulatory obligations. We therefore do not consider that any amendments to paragraphs 8.16 to 8.18 of the Guidance are required.

Disclosure to skilled persons and skilled person's reports

8.24 Paragraph 8.3 of the Guidance states that, before we disclose information to a skilled person, we will carefully consider whether the information is relevant to the purpose of their report. Section 393 of the Communications Act applies to skilled persons too. The skilled person faces the same statutory confidentiality obligations as Ofcom and would be prohibited from disclosing confidential information except for specified purposes in specific circumstances.

8.25 For the avoidance of doubt, we recognise that skilled person's reports are likely to contain confidential information. Where we consider disclosure of information from a skilled person's report necessary (for example, when explaining our reasons for a Technology

[177] [✂] response to December 2024 Consultation, p.21.
[178] [✂] response to December 2024 Consultation, p.20.
[179] [✂] response to December 2024 Consultation, p.22.
[180] [✂] response to December 2024 Consultation, p.7.

Notice decision), we will follow the process in paragraphs 8.17 to 8.18 of the Guidance, giving the service provider an opportunity to make representations on confidentiality before publication.

Blanket confidentiality claims

8.26 Paragraph 8.18 of the Guidance states that Ofcom does not accept unsubstantiated blanket confidentiality claims. Further, as explained in paragraph 3.29 of Ofcom's Online Safety Information Powers Guidance, blanket claims of confidentiality covering entire documents or types of information are unhelpful and will rarely be accepted. Recipients should therefore identify specific words, numbers, phrases or pieces of information they consider to be confidential.

Notification period for confidentiality representations

8.27 We would expect service providers to make representations on confidentiality when they give information to Ofcom and would take account of this when preparing the text of website updates or media releases.

8.28 Insofar as any website updates or media releases contain information that a provider considers confidential, the process set out in paragraphs 8.16 to 8.18 of the Guidance would apply. The provider would therefore have a reasonable opportunity to make representations about confidentiality, and - for the avoidance of doubt - would have longer than a day to do so. This includes where Ofcom is proposing to disclose a Technology Notice in full (although, as noted in paragraph 8.7 of the Guidance, we do not generally expect to do this).

8.29 The purpose of the one-day advance notice referenced in paragraph 8.10 of the Guidance is not to give the provider an opportunity to identify if confidential information is contained in the website update or media release. Rather, it is to inform the service provider about imminent publication and provide it with an opportunity to prepare appropriate communications. This is why we do not agree the text of such updates with providers, and we note that this approach is consistent with our Online Safety Enforcement Guidance.[181]

[181] Paragraphs 5.19 and 8.29.

A1. Regulatory framework

A1.1 In this annex we provide an overview of the regulatory framework relevant to Ofcom's Technology Notice functions, to give some additional context to the matters discussed in the Technology Notices Guidance Statement.

A1.2 In particular, it explains:

a) Ofcom's powers under the Act to tackle illegal harms, and specifically terrorism and CSEA content;

b) our powers under section 121 of the Act, including the steps required and other considerations for Ofcom before we can issue a Technology Notice; and

c) Ofcom's general duties relevant to the exercise of our Technology Notice functions.

A1.3 The overview in this annex should not be considered as an exhaustive summary of the law in this area. Readers are advised to read the Act for this purpose.

Ofcom's powers to tackle terrorism and CSEA content

A1.4 The Act provides for a new regulatory framework which has the general purpose of making the use of regulated internet services safer for individuals in the UK. To achieve this, the Act imposes duties which require providers to identify, mitigate, and manage the risks of harm from illegal content and activity that is harmful to children, as well as conferring new functions and powers on Ofcom.

A1.5 The Act places a range of new duties on all providers of Part 3 services in relation to illegal content. The concept of 'illegal content' is discussed in more detail below. These duties differ depending on whether the service is a user-to-user or search service, and whether the content is priority illegal content or relevant non-priority illegal content. They can, however, broadly be broken down into two categories:

a) duties to assess risks of harm arising on the service, otherwise referred to as the 'risk assessment duties'; and

b) duties to manage and mitigate those harms, otherwise referred to as the 'illegal content safety duties'.

A1.6 A provider's illegal content safety duties will vary depending on whether they are providing a user-to-user service or a search service. For user-to-user services, these duties include:

a) to take or use proportionate measures relating to the design or operation of the service to prevent individuals from encountering priority illegal content and minimising the length of time that such content is present on the service;[182]

b) to take or use proportionate measures relating to the design or operation of the service to effectively mitigate and manage the risks of harm to individuals, as identified in the service provider's most recent illegal content risk assessment;[183] and

[182] Section 10(2)(a) and 10(3)(a) of the Act.
[183] Section 10(2)(c) of the Act.

c) to operate the service using proportionate systems and processes designed to swiftly take down (priority or non-priority) illegal content when they become aware of it. This is frequently referred to as the 'takedown duty'.[184]

A1.7 For regulated search services, these duties include:

a) to take or use proportionate systems and processes to effectively mitigate and manage the risks of harm to individuals, as identified in a service's most recent illegal content risk assessment;[185] and

b) to operate a service using proportionate systems and processes to minimise the risk of individuals encountering search content that is priority illegal content and other illegal content that the provider knows about.[186]

A1.8 Part 7 of the Act sets out Ofcom's powers and duties in relation to regulated services. These include a specific power under section 121 of the Act to issue 'notices to deal with' two specific types of illegal content – terrorism and/or CSEA content (see below) – where we consider it necessary and proportionate. We refer to this power as our Technology Notice power.

What are terrorism and CSEA content?

A1.9 Terrorism and CSEA content are both categories of 'priority illegal content' under the Act.

A1.10 'Illegal content' is a new concept created by the Act, defined as 'content that amounts to a relevant offence'.[187] Section 192 of the Act sets out how, where they are required to do so, providers of services should make judgements as to whether content is illegal content. The approach set out in the Act is such that 'illegal content judgements' are to be made if the service provider has 'reasonable grounds to infer' that the content in question amounts to a relevant offence.[188] 'Reasonable grounds to infer' is not a criminal threshold, and there are no criminal implications for the user if their content is judged to be illegal content against this threshold.[189]

A1.11 The Act sets out the 'relevant offences' in scope of the criminal law in the UK for the purposes of identifying 'illegal content'. Under the Act, the relevant offences comprise:

a) a list of priority offences, and

b) 'non-priority' (or 'other') offences.

---

[184] Section 10(3)(b) of the Act.
[185] Section 27(2) of the Act.
[186] Sections 27(3)(a) and 27(3)(b) of the Act.
[187] Content consisting of certain words, images, speech or sounds will amount to an offence if (a) the use of the words, images, speech or sounds amounts to a relevant offence, (b) the possession, viewing or accessing of the content constitutes a relevant offence, or (c) the publication or dissemination of the content constitutes a relevant offence. A full definition of illegal content may be found in section 59 of the Act.
[188] The service must make this judgement using all 'relevant information that is reasonably available' to it. These two principles are more fully explained in our Illegal Content Judgements Guidance (the ICJG). This guidance is designed to help providers better understand what illegal content is and how they should make judgements about that content.
[189] The provider is not obliged to report illegal content to law enforcement except where the content in question is subject to requirements to report Child Sexual Exploitation and Abuse (CSEA) material to the National Crime Agency (NCA) in the UK, as set out in section 66 of the Act.

A1.12 In total there are over 130 priority offences in scope of the Act. These are set out in Schedules 5 (Terrorism offences), 6 (CSEA offences) and 7 (Priority offences) to the Act and are the most serious offences covered by the Act, as defined by Parliament. All providers of Part 3 services will need to act to prevent users encountering content amounting to one of these offences.

A1.13 Terrorism content refers to content which amounts to an offence specified in Schedule 5 to the Act. These offences include, but are not limited to:

a) A series of offences relating to 'proscribed organisations';

b) Offences related to information likely to be of use to a terrorist;

c) Offences relating to training for terrorism;

d) Other offences involving encouraging terrorism or disseminating terrorist materials;

e) Miscellaneous, more specific terrorism offences; and

f) Offences relating to financing terrorism.

A1.14 CSEA content refers to content which amounts to an offence specified in Schedule 6 to the Act. These offences include, but are not limited to:

a) Offences relating to the making, showing, distributing or possessing of an indecent image or film of a child;

b) An offence of possession of a prohibited image of a child;

c) Linking to or directing a user to child sexual abuse material (CSAM);

d) An offence of possession of a paedophile manual;

e) An offence of publishing an obscene article;

f) Sexual activity offences (potential victim under 16);

g) Adult to child offences (potential victim under 16);

h) 'Arranging' together with 'assisting', 'encouraging' and 'conspiring' offences which could take place between adults and/or children (potential victim(s) under 16); and

i) Offences concerning the sexual exploitation of children and young people aged 17 or younger.

Ofcom's Technology Notice powers within the wider Illegal Harms Framework

Ofcom's powers in respect of Codes of Practice

A1.15 Codes of Practice provide the foundation for Ofcom's implementation of the online safety regime in the UK. As required by the Act, they set out Ofcom's recommendations to regulated services about the measures they may take to be treated as complying with their new online safety duties, including their illegal content safety duties.

A1.16 While service providers are not required to follow the Codes, those that do will be treated as compliant with the relevant duties.[190] Services may also take what the Act calls

[190] Section 49(1) of the Act.

'alternative measures' but must keep a record of the action they take and explain how this meets the relevant safety duties.

A1.17 Ofcom can include a range of measures within Codes of Practice relating to the design and operation of regulated services. These can include, but are not limited to, measures relating to regulatory compliance and risk management, the design of functionalities, algorithms and other features, policies on terms of use, user support measures and content moderation measures.

A1.18 The measures included within Codes of Practice are not targeted at individual regulated services. They are intended to apply either to all regulated user-to-user or search services or to specific kinds of services based on their size and capacity, and the findings of their most recent risk assessment. The Act also sets out principles that Ofcom must have regard to in preparing its Codes of Practice, including the principle that the measures included must be proportionate and technically feasible.[191]

A1.19 Ofcom is also able to recommend the use of 'proactive technology' as a way of complying with some of the duties set out in the Act, including the illegal content safety duties. Proactive technology includes some kinds of content identification technology, user profiling technology and behaviour identification technology.[192] There are, however, additional constraints on Ofcom's power to include proactive technology measures in a Code of Practice. Importantly, Ofcom may not recommend the use of proactive technology to analyse user-generated content communicated privately, or metadata relating to such content.[193]

Ofcom's first Illegal Content Codes of Practice

A1.20 Our first Illegal Content Codes of Practice,[194] which came into force on 17 March 2025, include a range of measures that will help make the use of internet services safer for UK individuals and reduce the prevalence and dissemination of priority illegal content, including terrorism and CSEA content, online. These include that the providers of regulated Part 3 services:

a) Set clear and accessible terms and conditions that explain how users will be protected from illegal content, including terrorism and CSEA content.

b) Design content moderation systems to swiftly take down illegal content of which it is aware (that may be terrorism or CSEA content). When setting prioritisation policies for content moderation systems, providers should factor in, among other things, the number of UK users encountering a particular item of illegal content and the severity of harm from that content.

c) Adequately resource and train content moderation teams to deal with terrorism and CSEA content, including to meet increases in demand caused by external events, such as crises and conflicts.

d) Have user reporting and complaints processes for illegal content that are easy to find, access and use.

---

[191] Paragraph 2(c) of Schedule 4 to the Act.
[192] Section 231 of the Act.
[193] Paragraph 13(4) of Schedule 4 to the Act.
[194] See our Illegal content Codes of Practice for user-to-user services and Illegal content Codes of Practice for search services.

e) Remove accounts if there are reasonable grounds to infer they are run by or on behalf of a terrorist organisation proscribed by the UK Government.

f) Take measures to tackle the online grooming of children, including safer default settings that make it harder for strangers to find and interact with children online.

g) Search services should take appropriate moderation action in relation to terrorism content, such as making sure this content is de-indexed or de-prioritised.

h) Provide supportive prompts and messages for child users during their online journey, to empower them to make safe choices online, such as when they turn off default settings or receive a message from a user for the first time.

A1.21 The first Illegal Content Codes of Practice also include the following proactive technology measures for certain Part 3 services:[195]

a) Use of hash-matching technology, which automatically detects known CSAM images shared by users in their public content.

b) Use of Uniform Resource Locator (URL) detection technology, which scans public posts to remove illegal URLs that lead to material depicting the sexual abuse of children.

c) Prevention of CSAM URLs from appearing in results by search engines and applying warning messages on search services when users search for content that explicitly relates to CSAM.

A1.22 Code measures recommending the use of proactive technology to detect and/or 'take down' illegal content share some features with our Technology Notice powers under the Act. This is because, for example, a Technology Notice could require a regulated user-to-user service to use accredited technology to identify, and swiftly take down, certain types of illegal content. As with preparing its Codes of Practice, Ofcom must also consider whether it is proportionate to give a Technology Notice and have regard to the matters set out in the Act.[196] It is also important to note that, although not required to under the Act, we have said in our Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023 (the Guidance) that we will consider the technical feasibility for the service provider of doing what would be required of them in the Technology Notice, taking into account the way the service is configured, when considering whether it is necessary and proportionate to issue a Notice.[197]

Ofcom's powers in relation to Technology Notices

A1.23 We have already explained, in section 2 of the Technology Notices Guidance Statement, that Ofcom's additional powers under section 121 of the Act are intended to complement

[195] In June 2025, Ofcom launched a consultation setting out proposals for a series of additional safety measures for Part 3 services to further strengthen our first Illegal Content Codes of Practice. These include proposed measures relating to proactive technology, such as to recommend that providers assess whether proactive technology that is sufficiently accurate, effective and free from bias exists that could be used to identify a range of harms on their service (including CSEA content, such as image-based CSAM and CSAM URLs) and if so deploy that technology, the use of hash-matching technology to detect and remove intimate image abuse content and terrorism content, and to increase the number of providers in scope of an existing measure recommending the use of hash-matching technology for CSAM. The consultation closed in October 2025. We are considering consultation responses, and we will publish our statement by Autumn 2026.

[196] Section 124 of the Act.

[197] Paragraph 3.8 of the Guidance.

its power to recommend measures in Codes of Practice and enforce against non-compliance with the illegal content safety duties.

A1.24 We also provided an overview of some important ways in which Ofcom's power to require the use of a technology through Technology Notices differs from our power to recommend measures in a Code of Practice. We do not repeat these in this Annex but have provided a more detailed overview of the statutory provisions relevant to our powers under section 121 of the Act below.

Ofcom's Technology Notice powers

Who Ofcom can give a Technology Notice to

A1.25 Ofcom can only give a Technology Notice to the provider of:

a) a 'regulated user-to-user service', which means an internet service through which content that is generated, uploaded or shared by users may be encountered by other users of the service;[198]

b) a 'regulated search service', which means an internet service that is, or includes, a search engine;[199] or

c) a 'combined service', which is a regulated user-to-user service that includes a public search engine.[200]

A1.26 Such services will be 'regulated' if they have 'links with the United Kingdom'[201] and do not fall within Schedule 1 or Schedule 2 to the Act.[202] A service has links with the UK if it has a significant number of UK users or if UK users form one of the target markets (or the only target market).[203] A service will also be considered to have links to the UK if it is capable of being used in the UK by individuals, and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK presented by user-generated content present on the service or search content of the service.[204]

A1.27 We refer to these as 'Part 3 services' and providers of such services as 'Part 3 service providers' (or 'service providers') in the Technology Notices Guidance Statement.[205]

What Ofcom can require in a Technology Notice

A1.28 The Act provides Ofcom with the power,[206] if we consider it necessary and proportionate, to give a Technology Notice to a Part 3 service provider requiring it to:

[198] Section 3(1) of the Act.
[199] Section 3(4) of the Act.
[200] Section 4(7) of the Act.
[201] Section 4(2)(a) of the Act.
[202] Section 4(2)(b) of the Act.
[203] Section 4(5) of the Act.
[204] Section 4(6) of the Act.
[205] Regulated user-to-user and regulated search services are defined in the Act as 'Part 3 Services' because Part 3 of the Act imposes duties on providers of these services. We have adopted this definition throughout this document.
[206] Section 121(1) of the Act.

use accredited technology to deal with terrorism content and/or CSEA content (or 'relevant content'); or

use best endeavours to develop or source technology which meets minimum standards of accuracy to deal with CSEA content.

A1.29 Where we refer to 'accredited technology', we mean technology that has been accredited by Ofcom (or another person appointed by Ofcom) as meeting minimum standards of accuracy in the detection of relevant content.[207] The 'minimum standards of accuracy' are standards approved and published by the Secretary of State following advice by Ofcom.[208]

A1.30 Subject to paragraph A1.33 below, a Notice requiring the use of accredited technology may require the providers of:

a) regulated user-to-user services to use that technology to identify and swiftly take down, or prevent individuals from encountering, terrorism content and/or CSEA content;[209] and

b) regulated search services to use that technology to identify search content of the service that is relevant content and swiftly take measures to secure that, so far as possible, search content no longer includes such content identified by the technology.[210]

A1.31 A requirement to use accredited technology may be complied with by use of the technology alone or by means of the technology together with the use of human moderators.[211]

A1.32 For a Notice relating to the development or sourcing of technology, Part 3 services may be required to use best endeavours to develop or source technology which meets minimum standards of accuracy and can be used:

a) in the case of regulated user-to-user services, to identify and swiftly take down, or prevent individuals encountering, CSEA content communicated publicly and privately;[212] and

b) in the case of regulated search services, to identify search content of the service that is CSEA content and swiftly take measures to secure that, so far as possible, search content no longer includes CSEA content identified by the technology.[213]

A1.33 For regulated user-to-user services, we can require them to use accredited technology, or to develop or source technology, to address CSEA content communicated both privately and publicly by means of the service. However, a Notice requiring the use of accredited technology to address terrorism content can only require the use of that technology to address content communicated publicly by means of the service.[214]

---

[207] Section 125(12) of the Act.
[208] Section 125(13) of the Act.
[209] Section 121(2)(a) of the Act.
[210] Section 121(3)(a) of the Act.
[211] Section 121(5) of the Act.
[212] Section 121(2)(b) of the Act.
[213] Section 121(3)(b) of the Act.
[214] Section 232 of the Act specifies the following factors which we must, in particular, consider when deciding whether content is communicated 'publicly' or 'privately' for the purposes of a Technology Notice to deal with terrorism content: a) the number of individuals in the UK who are able to access the content by means of the

A1.34 A Notice may require a combined service to do any, or a combination, of the things described above in relation to the user-to-user part and/or search engine function of the service.[215]

A1.35 We may impose requirements in a Technology Notice only in relation to the design and operation of a Part 3 service in the UK, or as it affects UK users of the service.[216]

Additional requirements

A1.36 Where we issue a Technology Notice requiring the use of accredited technology, it is taken to require the service provider to make such changes to the design or operation of the service as are necessary for the accredited technology to be used effectively.[217]

A1.37 If a service provider is already using accredited technology in relation to the service, we may require that the service provider use the accredited technology more effectively and specify how that must be done.[218]

A1.38 A Technology Notice may also require the service provider to operate an effective complaints procedure, which:

a) in the case of a user-to-user service (or user-to-user part of a combined service), allows for UK users to challenge the provider for taking down content which they have generated, uploaded or shared on the service;[219]

b) in the case of a search service (or search engine of a combined service), allows for an interested person to challenge measures taken or in use by the service provider that result in content relating to that interested person no longer appearing in search results of the service.[220]

Steps and considerations for Ofcom before issuing a Technology Notice to a particular Part 3 service provider

A1.39 We have already set out, at paragraphs 2.17 and 2.18 of the Technology Notices Guidance Statement, some important steps that need to have been taken before Ofcom can consider issuing a Technology Notice. However, there are several additional steps and considerations within the Act that Ofcom must follow in an individual case before we can issue a Technology Notice to a particular Part 3 service provider.

---

service; b) any restrictions on who may access the content by means of the service; and c) the ease with which content may be forwarded to or shared with users of the service other than those who originally encounter it, or users of another internet service. See also Ofcom's Guidance on content communicated 'publicly' and 'privately'.

[215] Section 121(4) of the Act.

[216] Section 125(10) of the Act.

[217] Section 125(5) of the Act. See also paragraph 598 of the Explanatory Notes to the Act, which explains that such changes must be proportionate.

[218] Section 125(2) of the Act.

[219] Section 125(3) of the Act.

[220] Section 125(4) of the Act. 'Interested person' means a person that is responsible for a website or database capable of being searched by the search engine, provided that: a) in the case of an individual, the individual is in the UK; b) in the case of an entity, the entity is incorporated or formed under the law of any part of the UK (section 227(7) of the Act).

Skilled person's report

A1.40 Before we may issue a Technology Notice, Ofcom is required to obtain a report from a skilled person, appointed by us, to assist us in deciding whether to give a Notice, and to advise about the requirements that might be imposed. A 'skilled person' means a person appearing to Ofcom to have the skills necessary to prepare a report about matters relevant to those purposes.[221]

Warning Notice

A1.41 We must give a Warning Notice to the service provider before we may issue a Technology Notice. Section 123 of the Act sets out the information that we must include in a Warning Notice depending on whether it relates to the use of accredited technology[222] or to the development or sourcing of technology.[223] In either case, a Warning Notice must provide the service provider with an opportunity to make representations to Ofcom on our intention to issue a Technology Notice.[224]

Ofcom must be satisfied that a Technology Notice is necessary and proportionate

A1.42 Section 124 of the Act set out the matters which we must particularly consider when deciding whether it is necessary and proportionate to issue a Technology Notice. These are:

a) the kind of service it is;

b) the functionalities of the service;[225]

c) the user base of the service;

d) in the case of a notice relating to a user-to-user service (or to the user-to-user part of a combined service), the prevalence of relevant content on the service, and the extent of its dissemination by means of the service;

e) in the case of a notice relating to a search service (or to the search engine of a combined service), the prevalence of search content of the service that is relevant content;

f) the level of risk of harm to individuals in the United Kingdom presented by relevant content, and the severity of that harm;[226]

g) the systems and processes used by the service which are designed to identify and remove relevant content;[227] and

h) the contents of the skilled person's report.

A1.43 Where we are considering issuing a Notice requiring the use of **accredited technology**, we must also consider:

---

[221] Sections 122 and 104(3), (4) and (6)(a) of the Act.
[222] Section 123(2) of the Act.
[223] Section 123(3) of the Act.
[224] Section 123(2)(f) and (g) and (3)(f) and (g) of the Act.
[225] 'Functionality' is defined in section 233 of the Act.
[226] See section 234 of the Act for the meaning of 'harm'.
[227] 'Systems and/or processes' refers to human or automated systems and/or processes, including technologies (section 236(1) of the Act).

a) the extent to which the use of the specified technology would or might result in interference with users' right to freedom of expression within the law;[228] and

b) the level of risk of the use of the specified technology resulting in a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of the service (including, but not limited to, any such provision or rule concerning the processing of personal data); and

c) in the case of a notice relating to a user-to-user service (or to the user-to-user part of a combined service), the extent to which the use of the specified technology would or might have an adverse impact on the availability of journalistic content on the service,[229] or result in a breach of the confidentiality of journalistic sources; and

d) whether the use of any less intrusive measures than the specified technology would be likely to achieve a significant reduction in the amount of relevant content.

What information must Ofcom include in a Technology Notice

A1.44 Section 125 of the Act specifies information that must be included in a Technology Notice depending on whether the Notice relates to the use of accredited technology or to the development or sourcing of technology. We have provided further detail on some of the information we are required to provide below.

Timescales for compliance

A1.45 In the case of a Technology Notice to use **accredited technology**, we must specify:

a) a reasonable period for compliance with the Notice;[230] and

b) the period within which the requirements imposed by the Notice will have effect.[231] This may be for up to 36 months from the last day of the period for compliance (set out at a) above).[232]

A1.46 Where we issue a Technology Notice relating to the **development or sourcing of technology**, the Notice must specify a reasonable period within which each of the steps specified in the Notice must be taken.[233] We must take into account the size and capacity of the service provider, and the state of development of technology capable of achieving the purpose for which the technology is to be developed or sourced, in deciding what period(s) to specify.[234]

Review of a Technology Notice

A1.47 We must carry out a review of the service provider's compliance with the Technology Notice before the end of the period for which the Notice has effect or, in the case of a Notice to develop or source technology before the last date by which any step specified in

[228] 'Freedom of expression' means the freedom to receive and impart ideas, opinions or information (referred to in Article 10(1) of the European Convention on Human Rights) by means of speech, writing or images (section 236(1) of the Act).
[229] See section 19 of the Act for the meaning of 'journalistic content'.
[230] Section 125(6)(e) of the Act.
[231] Section 125(6)(f) of the Act.
[232] Section 125(7) of the Act.
[233] Section 125(8)(d) of the Act.
[234] Section 125(9) of the Act.

the Notice is required to be taken.[235] A Technology Notice must contain information about when Ofcom intends to review the Notice.

Guidance for Part 3 Providers

A1.48 Ofcom must produce, and publish, guidance for Part 3 service providers about how we propose to exercise our functions under Chapter 5 of Part 7 of the Act (our 'Technology Notice functions') and keep it under review. We must have regard to the Guidance when exercising, or deciding whether to exercise, those functions.[236] See Ofcom's Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023.

Annual Report

A1.49 Ofcom must also produce and publish an annual report about the exercise of our Technology Notice functions and technology which is in the process of development so as to meet, minimum standards of accuracy. Ofcom must send a copy of our annual report to the Secretary of State, who must lay it before Parliament.[237]

A1.50 A copy of Ofcom's most recent Annual Report on Notices to deal with terrorism content and/or CSEA content can be found on our website.

General duties

A1.51 In addition to the specific duties and considerations summarised above, Ofcom has a range of general statutory duties that are relevant to the exercise of its Technology Notice functions.

A1.52 Specifically, when exercising those functions, we will act in accordance with our principal duty under section 3(1) of the Communications Act 2003 (the Communications Act):

a) to further the interests of citizens in relation to communications matters; and

b) to further the interests of consumers in relevant markets, where appropriate by promoting competition.

A1.53 In performing our principal duty, Ofcom must have regard to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent, and targeted only at cases in which action is needed, as well as any other principles appearing to us to represent best regulatory practice.[238] In terms of our Technology Notice functions, this means we will take action where it is proportionate and appropriate, but with a willingness to intervene firmly, promptly, and effectively where required. We will always seek the least intrusive regulatory methods to achieve our objectives and ensure that interventions are evidence-based, proportionate, consistent, accountable and transparent in both deliberation and outcome, in line with our regulatory principles.

[235] Section 126(4) of the Act.
[236] Section 127 of the Act.
[237] Section 128 of the Act.
[238] See section 3(3) of the Communications Act.

A1.54 In addition, we are required to secure a number of objectives including the adequate protection of citizens from harm presented by content on regulated services, through the appropriate use by providers of such services of systems and processes designed to reduce the risk of such harm.[239] In our work to secure this objective, we must have regard to the matters in section 3(4A) of the Communications Act to the extent they appear to us relevant, which include (among other things):

a) the risk of harm to citizens presented by regulated services;

b) the need for a higher level of protection for children than for adults;

c) the desirability of promoting the use by providers of regulated services of technologies which are designed to reduce the risk of harm to citizens presented by content on regulated services; and

d) the need to exercise our functions so as to secure that providers of regulated services may comply with such duties by taking measures, or using measures, systems or processes, which are (where relevant) proportionate to: (i) the size or capacity of the provider in question, and (ii) the level of risk of harm presented by the service in question, and the severity of the potential harm.

A1.55 Section 3(4) of the Communications Act also sets out other matters to which Ofcom should have regard, including the vulnerability of children and of others whose circumstances appear to put them in special need of protection and the desirability of preventing crime and disorder.

A1.56 In exercising our regulatory functions, we are also required to have regard to the desirability of promoting economic growth (the Growth Duty).[240] In particular, we must consider the importance for the promotion of economic growth of exercising the regulatory function in a way which ensures that regulatory action is taken only when it is needed, and any action taken is proportionate. Section 110(3) of the Deregulation Act 2015 requires us to have regard to the Growth Duty: Statutory Guidance.

A1.57 Under section 92(2) of the Act, when carrying out our online safety functions, we must also have regard to the Statement of Strategic Priorities (SSP) that has been designated by the Secretary of State under section 172(1) of the Act, pursuant to the requirements set out in section 173.[241]

A1.58 As a public authority, Ofcom must also act in accordance with its public law duties to act lawfully, rationally and fairly and, under section 6 of the Human Rights Act 1998, it is unlawful for Ofcom to act in a way which is incompatible with the European Convention on Human Rights ('the ECHR'). Of particular relevance to Ofcom's functions under the Act are the right to freedom of expression (Article 10 ECHR) and the right to privacy (Article 8 ECHR). Other ECHR rights which may also be relevant are the right to freedom of thought, conscience and religion (Article 9 ECHR) and the right to freedom of assembly and

[239] Section 3(2)(g) of the Communications Act.
[240] Section 108 of the Deregulation Act 2015, which was extended to Ofcom's online safety functions by the Economic Growth (Regulatory Functions) (Amendment) Order 2024 with effect from 6 April 2026.
[241] On 2 July 2025, the Secretary of State designated its SSP for Online Safety (the 2025 SSP). This is available at: Statement of Strategic Priorities for Online Safety - GOV.UK. As at the date of this statement, we have a duty to have regard to the 2025 SSP in carrying out our online safety functions.

association (Article 11 ECHR). In particular, any interference must be prescribed by or in accordance with the law, pursue a legitimate aim and be necessary in a democratic society.

A1.59 In order to be 'necessary', the restriction must be proportionate to the legitimate aim pursued and correspond to a pressing social need. The relevant legitimate aims that Ofcom acts in pursuit of in the context of our functions under the Act include the prevention of crime and disorder, public safety and the protection of health and morals, and the protection of the rights and freedoms of others.[242] In this context, Parliament has legislated for terrorism and CSEA content to be designated as 'priority illegal content' under the Act, requiring service providers to use proportionate systems and processes designed to minimise the length of time for which it is present, and providing for Technology Notices to be issued where necessary and proportionate. This reflects the substantial public interest in limiting the risks of harm to individuals in the UK from this content, and, in relation to CSEA content in particular, the rights of children not to be subject to such abuse and harm.

A1.60 Ofcom is also subject to duties under the Equality Act 2010 (the EA 2010). This includes the public sector equality duty set out in section 149, which requires Ofcom, in the exercise of our functions, to have due regard to the need to:

a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the EA 2010;

b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; and

c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

A1.61 The relevant protected characteristics are age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

A1.62 In addition, section 75 of the Northern Ireland Act 1998 (the NI Act) requires us to promote good relations between people sharing specified characteristics, including people of different religious beliefs, political opinions or racial groups.

[242] Articles 8(2), 9(2), 10(2) and 11(2) ECHR.

A2. Impact Assessments

Impact Assessment under section 7 of the Communications Act

A2.1 Section 7 of the Communications Act requires us to carry out and publish an assessment of the likely impact of implementing a proposal which would be likely to have a significant impact on businesses or the general public, or when there is a major change in Ofcom's activities. In accordance with section 7(4B) of the Communications Act, we also have to consider the likely impact on small and micro businesses in relation to proposals connected with our online safety functions. As a matter of policy Ofcom is committed to carrying out and publishing impact assessments in relation to the great majority of our policy decisions, although the form of that assessment will depend on the particular nature of the proposal.

A2.2 We published an impact assessment based on the proposals set out in our December 2024 Consultation (see Annex 7 of the consultation document). We have now updated that impact assessment to include consideration of stakeholder feedback received during the consultation and our Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023.

A2.3 The purpose of this impact assessment is to consider the impact of proposals over which we have regulatory discretion, rather than impacts that are unavoidable due to the nature of the duties in the Act. Therefore, this impact assessment does not consider the potential impact of Ofcom's power to issue a Technology Notice as this power has been conferred on Ofcom by Parliament and has been subject to impact assessments through the legislative and policy making process. It also does not consider the potential impact from Ofcom being required to provide guidance to the providers of Part 3 services about how we propose to exercise our Technology Notice functions. We are required by the Act to do so.

A2.4 We do however have discretion on the substance of our guidance to the providers of Part 3 services. This impact assessment will therefore assess the likely impact from our Guidance.

A2.5 In the context of our impact assessment, we have also considered the potential impacts of our Guidance on economic growth and, in terms of the 2025 SSP, we have had regard to the following priority areas in particular: safety by design, agile regulation and technology and innovation.

A2.6 The scale of the impact will depend on a range of factors. These include, but are not necessarily limited to: the current state of the market for terrorism and CSEA content detection technologies and the scale of interest from that market in seeking accreditation; the extent to which the minimum standards of accuracy ultimately approved and published by the Secretary of State resemble those recommended by Ofcom in the advice to the Secretary of State; what technology, if any, is ultimately accredited against those standards; and to which services, if any, we are considering issuing (and/or we issue) a Technology Notice.

A2.7 Although Ofcom is required to provide advice to the Secretary of State regarding minimum standards of accuracy in the detection of terrorism content and CSEA content, it is ultimately for the Secretary of State to determine the minimum standards of accuracy which are approved and published. Only once these have been published will Ofcom (or a person appointed by Ofcom as relevant) be able to consider whether a particular

technology can be accredited as meeting those minimum standards, and if so, whether to issue a Technology Notice to a particular service provider. Given the above, we are unable to estimate the specific impacts to Part 3 regulated services, providers of terrorism and/or CSEA content detection technologies, or the safety outcomes for users of Part 3 services regulated under the Act in aggregate from the Guidance.[243]

Stakeholder feedback on our impact assessment

A2.8 We did not receive any explicit comments from stakeholders about our impact assessment for the Guidance. However, we recognise that a large number of the comments provided by respondents were about the impacts in general of our draft guidance and we have been mindful of this when finalising our impact assessment below. Overall, however, our impact assessment remains broadly unchanged from the provisional assessment set out in our December 2024 Consultation.

Impact on Part 3 regulated services

A2.9 We do not anticipate that the Guidance in itself should have any direct impacts on the providers of Part 3 services, including on small or micro businesses.

A2.10 Any impacts on specific Part 3 service providers would arise if and when Ofcom is considering issuing a Technology Notice to a particular provider. Before issuing a Technology Notice to a service provider in a particular case however, Ofcom would need to be satisfied that it is necessary and proportionate to require the technology to be used (or to be developed or sourced) and obtain a skilled person's report to help inform its view. We would also first issue a Warning Notice to the service provider explaining why we are minded to issue a Technology Notice and the requirements we are considering imposing, as well as give them the opportunity to make representations. As recognised in our Guidance, we would therefore consider the costs and impacts of imposing a Technology Notice on a particular Part 3 service provider before issuing a Technology Notice.

A2.11 While the Guidance explains how Ofcom proposes to exercise its Technology Notice functions, it is largely procedural and reflects the framework established by the Act. The Guidance is intended to benefit service providers by providing them with transparency on the steps we would expect to follow in making this assessment. As such, the Guidance does not in itself impose any additional burdens on the providers of Part 3 services, including small and micro businesses. Rather, by explaining our approach, it is intended to assist service providers in understanding how we propose to exercise our Technology Notice functions and therefore should help to reduce the future burden on them as to what the exercise of those functions might involve. Providing clarity about the matters that will inform the exercise of our Technology Notice functions might also encourage/incentivise appropriate investment by service providers. We therefore do not consider we need to separately consider the costs the Guidance might pose on businesses.

A2.12 When considering issuing a Technology Notice, we will also have regard to the regulatory principles of transparency, accountability, proportionality, consistency, and our interventions will be targeted only at cases in which action is needed, as described in paragraph 2.32 of our Guidance.

[243] This is in line with the Department for Science, Innovation & Technology's Impact Assessment of the Online Safety Act: Online Safety act enactment impact assessment, page 83.

Impact on the market for Terrorism and/or CSEA content detection technologies and the impact on technology providers

A2.13 We received feedback from one group of stakeholders that Ofcom should consider not only the proportionality of issuing a Technology Notice to an individual service's finances but also the market-level impact, noting there is a real risk of negative impact on UK digital services investment and innovation. [244]

A2.14 As noted from paragraph 3.55 of the Technology Notices Guidance Statement, it is not clear what this group of stakeholders mean by "the market in UK digital services". To the extent they are concerned about the impact on developers of trust and safety technology, and that Technology Notices and/or the wider online safety regime might drive investment to alternative jurisdictions, then we have explained in paragraph 3.56 of the Technology Notices Guidance Statement why we disagree, including that we expect our Technology Notice functions to promote competition and growth, and encourage investment and innovation in trust and safety technology. We also do not consider that our guidance itself will have any adverse direct impacts on the market for safety technologies. Indeed, it should have a positive impact insofar as it recognises that (where appropriate) we would consider giving a service provider to whom a Technology Notice is issued flexibility to choose between different accredited technologies in order to comply with the Technology Notice.

Impact on safety outcomes for users of Part 3 services

A2.15 We do not anticipate that the Guidance in itself should have any direct impacts on the users of Part 3 services. We do not reach a view in the Guidance on the circumstances in which it would be necessary and proportionate to issue a Technology Notice to a particular provider. Any decision on whether it is necessary and proportionate to issue a Technology Notice in a particular case would take account (as required by the Act) of the impacts on users, including in relation to freedom of expression within the law and privacy, as well as users' rights to be protected from harm.

A2.16 We recognise that there is a risk that no technologies are accredited. This would mean that we could not issue a Technology Notice requiring the use of technology. However, this risk exists irrespective of our Guidance. Further, we have taken this into account in our Advice to the Secretary of State by seeking to ensure that Ofcom can, if there are suitably accurate technologies, accredit these technologies. We have done this by ensuring that these standards reflect market capabilities and are sufficiently flexible.

Impact on rights

A2.17 As explained in paragraph A1.58 above, Ofcom is required by section 6 of the Human Rights Act 1998 to act in a way which is compatible with the ECHR. We recognise that the use of terrorism and/or CSEA content detection technologies in practice could have significant impacts on users' rights (including to freedom of expression and to privacy), as well as the rights of others.

[244] Drs Shurson, Keenan, Ó Floinn response to December 2024 Consultation, p.8.

A2.18 Our Guidance explains that we will have careful regard to rights impacts, taking account of all available evidence on a case-by-case basis, before issuing a Technology Notice. For example:

a) While not required by the Act, it recognises that we would typically expect to consider users' rights to freedom of expression, and the risk of an accredited technology resulting in a breach of any relevant statutory provision or rule of law concerning privacy, before issuing a Technology Notice relating to the development or sourcing of technology.

b) It also recognises that other ECHR rights may be relevant before issuing a Technology Notice. These include for example, the right to freedom of thought, conscience and religion and the right to freedom of assembly and association, as well as the right to privacy of victims of child sexual abuse and to the protection of their personal data.

c) The guidance provides transparency about how we will approach our assessment of whether a Technology Notice is necessary and proportionate. It explains that we would carefully consider the precise requirements that are imposed in any particular case, including the kinds of content or parts of the service on which any accredited technology is required to be used, and the wider systems and processes that might be required, such as complaints and human moderation. It also explains that we would consider whether compatibility testing is appropriate to inform our assessment.

Equality legislation and Welsh language

Equality Impact Assessment

A2.19 We received no specific feedback relating to the equality impact assessment included in our December 2024 Consultation. Nonetheless, we have considered the equality impact of our Guidance in light of the amendments made in response to stakeholder feedback, and we consider that our assessment of the impact remains unchanged.

A2.20 We have given careful consideration to whether our Guidance will have a particular impact on persons sharing protected characteristics (broadly including race, age, disability, sex, sexual orientation, gender reassignment, pregnancy and maternity, marriage and civil partnership and religion or belief in the UK and also dependents and political opinion in Northern Ireland), and in particular whether it may discriminate against such persons or impact on equality of opportunity or good relations. This assessment helps us comply with our duties under the EA 2010 and the NI Act.

A2.21 We do not consider our Guidance will in itself have any adverse equality impacts, as we are not requiring the use (or development or sourcing) of any technologies. Rather, our Guidance aims to provide stakeholders with an understanding of how Ofcom proposes to exercise our Technology Notice functions by setting out our general approach to exercising those functions, including the typical process we will follow for issuing a Notice.

A2.22 We would expect to consider equality impacts as part of any decision on whether it is necessary and proportionate to issue a Technology Notice to a particular provider, and what requirements should be imposed in that case. In particular, our Guidance:

a) explains that (see paragraphs 2.39 to 2.41);

b) acknowledges that individuals' rights under the EA 2010 may also be relevant to our consideration of whether it is necessary and proportionate to issue a Technology Notice (and, if so, what requirements to include) (see paragraph 3.9(c)).

Welsh Language Impact Assessment

A2.23 The Welsh Language (Wales) Measure 2011 made the Welsh language an officially recognised language in Wales. This legislation also led to the establishment of the office of the Welsh Language Commissioner who regulates and monitors our work. Certain public bodies, including Ofcom, are required to comply with Welsh Language Standards.[245] Accordingly, we have considered:

a) the potential impact of our Guidance on opportunities for persons to use the Welsh language;

b) the potential impact of our Guidance on treating the Welsh language no less favourably than the English language; and

c) how our Guidance could be formulated so as to have, or increase, a positive impact, or not to have adverse effects or to decrease any adverse effects.

A2.24 We received no specific feedback relating to the Welsh language impact assessment included in our December 2024 Consultation on our draft guidance. Nonetheless, we have considered the impact of our Guidance (including in light of the amendments made in response to stakeholder feedback), and we consider that our assessment of the impact remains unchanged.

A2.25 We do not consider our Guidance will have any adverse effect on the Welsh language nor treat the Welsh language less favourably than the English language. We also do not consider that it would be appropriate or proportionate for Ofcom to formulate its Guidance differently so as to have a positive impact on the Welsh language.

A2.26 However, we note that, as set out in our Technology Notices Advice Statement,[246] we are intending to ask those applying for accreditation to include details about the different languages supported by the technology. This would be used to inform any subsequent decisions on whether it is necessary and proportionate to require the use of that technology in a Technology Notice, and the requirements that might be included in that Notice.

[245] The Welsh Language Standards with which Ofcom is required to comply are available on our website.
[246] See, in particular, the 'Accreditation application template' at Annex 8 of our Technology Notices Advice Statement.

A3. Glossary

A3.1 This glossary defines the terms we have used throughout this document and the associated annexes.

Term	Definition
Accreditation scheme	A process to be set up by Ofcom which enables technologies to be assessed (by Ofcom or another person appointed by Ofcom) against the minimum standards of accuracy.
Accredited technology	Technology that has been accredited by Ofcom (or another person appointed by Ofcom) as meeting the minimum standards of accuracy.
Accuracy (metric)	The proportion of all cases correctly predicted by a technology, calculated by dividing the number of correct predictions (true positives and true negatives) by the total number of predictions.
Act	The Online Safety Act 2023.
Codes of Practice (Codes)	The set of measures recommended by Ofcom for compliance with certain online safety duties, including the illegal content safety duties. Ofcom is required to prepare Codes of Practice under section 41 of the Act. Our Illegal Content Codes of Practice for user-to-user services and search services and Protection of Children Codes of Practice for user-to-user services and search services are published on our website.
Combined service	A regulated user-to-user service that includes a public search engine.
Content	Anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description.

Term	Definition
CSAM (child sexual abuse material)	A category of CSEA content, including in particular indecent or prohibited images of children (including still and animated images, and videos, and including photographs, pseudo-photographs and non-photographic images such as drawings). CSAM also includes other material that includes advice about grooming or abusing a child sexually or which is an obscene article encouraging the commission of other child sexual exploitation and abuse offences. Furthermore, it includes content which links or otherwise directs users to such material, or which advertises the distribution or showing of CSAM.
CSAM URL	For the purposes of Ofcom's first Illegal Content Codes of Practice, this means a URL at which CSAM is present, or a domain which is entirely or predominantly dedicated to CSAM (and for this purpose a domain is 'entirely or predominantly dedicated' to CSAM if the content present at the domain, taken overall, entirely or predominantly comprises CSAM, such as indecent images of children, or content related to CSEA content).
CSEA (Child Sexual Exploitation and Abuse)	Refers to offences specified in Schedule 6 to the Act, including offences related to CSAM and grooming. CSEA includes but is not limited to causing or enticing a child or young person to take part in sexual activities, sexual communication with a child and the possession or distribution of indecent images. This is discussed in more detail in paragraph A1.14 of Annex 1.
CSEA content	Refers to content that amounts to an offence specified in Schedule 6 to the Act.
Deployment	For the purpose of this document, this refers to an operational technology being put into use (or being considered for use) on a particular internet service. References to deploy shall be construed accordingly.
ECHR	The European Convention on Human Rights (incorporated into domestic law by the Human Rights Act 1998).
Encounter	In relation to content, means read, view, hear or otherwise experience content.

Term	Definition
False Negative	Incorrectly classifying a positive sample as negative.
False Negative Rate	The proportion of positive cases incorrectly predicted by a technology as negative cases, calculated by dividing the number of false negatives by the total number of actual positive cases (false negatives and true positives).
False Positive	Incorrectly classifying a negative sample as positive.
False Positive Rate	The proportion of negative cases incorrectly predicted by a technology as positive cases, calculated by dividing the number of false positives by the total number of actual negative cases (false positives and true negatives).
Guidance	Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023.
Hash	For the purposes of Annex 1, this means a hash value. This is a digital footprint of content, which can be used together with a hash-matching algorithm to identify content that has that same or a similar digital footprint. A hash is distinct from the content to which it relates.
Hash-matching / Hashing	This is a type of technology which can be used as a content moderation tool, including to detect illegal content. Broadly speaking, it is a process for detecting when users attempt to upload content which has previously been identified as being illegal or otherwise violative. It allows services to prevent the re-upload of illegal content. It involves matching a hash of a unique piece of known illegal content stored in a database with user-generated content. Hashing is an umbrella term for techniques to create fingerprints of files on a computer system. An algorithm known as a hash function is used to compute a hash from a file. Hash matching can be used to prevent the upload, download, viewing or sharing of illegal or harmful content.

Term	Definition
Illegal content	Content which amounts to a relevant offence. Content amounts to a relevant offence if: (a) the use of that content (i.e., words, images, speech or sounds) amounts to a relevant offence; (b) the possession, viewing or accessing of the content constitutes a relevant offence; or (c) the publication or dissemination of the content constitutes a relevant offence.
Illegal content safety duties	The duties in section 10 of the Act (user-to-user services) and section 27 of the Act (search services).
Illegal harm	Harms arising from illegal content and the commission and facilitation of priority offences.
Initial assessment	Where we identify potential compliance concerns, we will assess the issue and consider what action, if any, it may be appropriate to take. Where the issue concerns terrorism, and/or CSEA content on a service, we may consider whether it would be appropriate to issue a Technology Notice as part of our initial assessment.
Internet service	A service that is made available by means of the internet. This includes where it is made available by means of a combination of the internet and an electronic communications service ('Electronic communications service' has the same meaning as in section 32(2) of the Communications Act 2003).
Metadata	For the purpose of this document, this is a set of data that describes and gives information about other data used for content moderation.
Minimum standards of accuracy	Refers to the standards approved and published by the Secretary of State relating to the detection of terrorism and CSEA content, following advice from Ofcom.
Online Safety Enforcement Guidance	Ofcom's guidance on how we will normally approach enforcement under the Act.
OS Information Powers Guidance	Ofcom's guidance for service providers and other stakeholders about the use of our information gathering powers under the Act.
Part 3 service	Refers to a regulated user-to-user service or a regulated search service.
Priority illegal content	Content which amounts to a priority offence.

Term	Definition
Priority offences	The offences set out in Schedules 5 (Terrorism offences), 6 (CSEA offences) and 7 (Priority offences) to the Act.
Proactive technology	This consists of three types of technology: content identification technology, user profiling technology, and behaviour identification technology (subject to certain exceptions), as defined in section 231 of the Act.
Provider	The provider of a user-to-user service, or search service, is to be treated as being the entity that has control over who can use the user-to-user part of the service, or the operations of the search engine (and that entity alone). The provider of a combined service is to be treated as the entity that has control over both who can use the user-to-user part of the service and the operations of the search engine (and that entity alone). If no entity has such control but an individual or individuals do, the provider of the service is to be treated as being that individual or those individuals.
Regulated search service	An internet service that is, or includes, a search engine. Such services will only be 'regulated' if they have 'links with the United Kingdom' and do not fall within Schedule 1 or Schedule 2 to the Act – see section 4(2) of the Act for more detail.
Regulated user-to-user service	An internet service through which content that is generated, uploaded or shared by users may be encountered by other users of the service. Such services will only be 'regulated' if they have 'links with the United Kingdom' and do not fall within Schedule 1 or Schedule 2 to the Act – see section 4(2) of the Act for more detail.
Relevant content	Terrorism content or CSEA content or both those kinds of content (depending on the kind, or kinds, of content in relation to which the specified technology is to operate).
Relevant non-priority illegal content	Content which amounts to a relevant non-priority offence.

Term	Definition
Relevant non-priority offence	Offences under UK law which are not priority offences under Schedules 5, 6 or 7 to the Act, where: a. The victim or intended victim of the offence is an individual (or individuals); b. The offence is created by the Online Safety Act, another Act, an Order in Council or other relevant instrument. The effect of this is that offences created by the UK courts are not relevant non-priority offences, and offences created in the devolved Parliaments or Assemblies are only relevant non-priority offences if certain procedures are followed in their making; c. The offence does not concern the infringement of intellectual property rights, the safety or quality of goods, or the performance of a service by a person not qualified to perform it; and d. The offence is not an offence under the Consumer Protection from Unfair Trading Regulations 2008.
Relevant offences	All priority offences and relevant non-priority offences.
Search	Search by any means, including by input of text or images or by speech, and references to a search request are to be construed accordingly.
Search content	Content that may be encountered in or via search results of a search service. It does not include paid-for advertisements, news publisher content, or content that reproduces, links to, or is a recording of, news publisher content. Content encountered 'via search results' includes content encountered as a result of interacting with search results (for example, by clicking on them) and does not include content encountered as a result of subsequent interactions.
Search engine	A service or functionality which enables a person to search some websites or databases but does not include a service which enables a person to search just one website or database.

Term	Definition
Search results	Content presented to a user of a search service (or a user-to-user service that includes a search engine) by operation of the search engine in response to a search request made by the user.
Search service	An internet service that is, or includes, a search engine.
Skilled person	A person appearing to Ofcom to have the skills necessary to prepare a report about matters that Ofcom considers to be relevant. A skilled person could be an individual, a firm or an organisation.
Skilled person's report	A report prepared by a skilled person about matters that Ofcom considers to be relevant. Ofcom is required to obtain a skilled person's report before issuing a Technology Notice.
Specified matters	The Specified Matters are set out in section 124(2) of the Act. These are matters that Ofcom must particularly consider when deciding whether it is necessary and proportionate to issue a Technology Notice. This is discussed in more detail in paragraphs 3.3-3.7 of the Guidance.
Systems and/or processes	Refers to human or automated systems and/or processes and accordingly includes technologies.
Taking down (content)	Refers to any action that results in content being removed from a user-to-user service or being permanently hidden so users of the service cannot encounter it (and related expressions are to be read accordingly).
Target content	Refers, for content moderation purposes, to the kind (or kinds) of content that a technology is being used to detect. In the case of a Technology Notice, the target content would be terrorism content or CSEA content (or both).
Technology Notice (Notice)	Refers to a notice under section 121 of the Act requiring a provider of a Part 3 service to use: (a) accredited technology to deal with terrorism or CSEA content, or both, or (b) best endeavours to develop or source technology to deal with CSEA content.
Technology Notice functions	Ofcom's functions under Chapter 5 of Part 7 of the Act.

Term	Definition
Terrorism content	An offence specified in Schedule 5 to the Act, including but not limited to offences relating to proscribed organisations, encouraging terrorism, training and financing terrorism. This is discussed in more detail in paragraph A1.13 of Annex 1.
Terrorism/CSEA content detection technology	Technology to identify and prevent users encountering user-generated terrorism content or CSEA content, and/or to identify search content that is terrorism content or CSEA content.
URL (Uniform Resource Locator)	A reference that specifies the location of a resource accessible by means of the internet.
URL detection	This is a type of technology which can be used as a content moderation tool. Broadly speaking, it can involve a process of matching URLs to URLs previously identified as hosting illegal or harmful content on other services.
User data	Data provided by users, including personal data (e.g., data provided when a user sets up an account), or created, compiled or obtained by providers of regulated services and relating to users (e.g., data relating to when or where users access a service or how they use it).
User-generated content	Content (a) that is: (i) generated directly on the service by a user of the service, or (ii) uploaded to or shared on the service by a user of the service, and (b) which may be encountered by another user, or other users, of the service by means of the service.
User-to-user part (of a service)	In relation to a user-to-user service, means the part of the service on which content that is user-generated content in relation to the service is present.
User-to-user service	An internet service through which content that is generated, uploaded or shared directly on the service by users may be encountered by other users of the service.

Term	Definition
Warning Notice	Refers to a notice given to the provider of a Part 3 service under section 123 of the Act which explains that Ofcom intends to issue a Technology Notice. The provider may make representations to Ofcom on the Warning Notice. Ofcom is required to give a Warning Notice before it can issue a Technology Notice.