Accreditation for terrorism/CSEA content detection technology

Annexes 1-3: Regulatory Framework, Impact Assessment & Glossary

Statement

Published: 8th May 2026

Contents

Annexes

A1. Regulatory framework 3

A2. Impact Assessments 16

A3. Glossary 23

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 Advice 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;[1]

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;[2] and

[1] Section 10(2)(a) and 10(3)(a) of the Act.
[2] 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'.[3]

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;[4] 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.[5]

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'.[6] 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.[7] '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.[8]

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.

---

[3] Section 10(3)(b) of the Act.
[4] Section 27(2) of the Act.
[5] Sections 27(3)(a) and 27(3)(b) of the Act.
[6] 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.
[7] 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.
[8] 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.[9] Services may also take what the Act calls '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.[10]

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.[11] 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.[12]

Ofcom's first Illegal Content Codes of Practice

A1.20 Our first Illegal Content Codes of Practice,[13] 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.

---

[9] Section 49(1) of the Act.
[10] Paragraph 2(c) of Schedule 4 to the Act.
[11] Section 231 of the Act.
[12] Paragraph 13(4) of Schedule 4 to the Act.
[13] See our Illegal content Codes of Practice for user-to-user services and Illegal content Codes of Practice for search services.

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

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:[14]

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.[15] 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 that we will consider the technical feasibility for the service provider of doing what would be required of them in the Technology Notice when considering whether it is necessary and proportionate to issue a Notice.[16]

Ofcom's powers in relation to Technology Notices

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

[14] 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.

[15] Section 124 of the Act.

[16] Paragraph 3.8.

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;[17]

b) a 'regulated search service', which means an internet service that is, or includes, a search engine;[18] or

c) a 'combined service', which is a regulated user-to-user service that includes a public search engine.[19]

A1.26 Such services will be 'regulated' if they have 'links with the United Kingdom'[20] and do not fall within Schedule 1 or Schedule 2 to the Act.[21] 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).[22] 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.[23]

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 Advice Statement.[24]

What Ofcom can require in a Technology Notice

A1.28 The Act provides Ofcom with the power,[25] if we consider it necessary and proportionate, to give a Technology Notice to a Part 3 service provider requiring it to:

[17] Section 3(1) of the Act.
[18] Section 3(4) of the Act.
[19] Section 4(7) of the Act.
[20] Section 4(2)(a) of the Act.
[21] Section 4(2)(b) of the Act.
[22] Section 4(5) of the Act.
[23] Section 4(6) of the Act.
[24] 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.
[25] Section 121(1) of the Act.

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

b) 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.[26] The 'minimum standards of accuracy' are standards approved and published by the Secretary of State following advice by Ofcom.[27]

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;[28] 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.[29]

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.[30]

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;[31] 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.[32]

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.[33]

---

[26] Section 125(12) of the Act.
[27] Section 125(13) of the Act.
[28] Section 121(2)(a) of the Act.
[29] Section 121(3)(a) of the Act.
[30] Section 121(5) of the Act.
[31] Section 121(2)(b) of the Act.
[32] Section 121(3)(b) of the Act.
[33] 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 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,

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.[34]

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.[35]

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.[36]

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.[37]

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;[38]

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.[39]

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 paragraph 1.6 of the Technology Notices Advice 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.

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

---

or users of another internet service. See also Ofcom's Guidance on content communicated 'publicly' and 'privately'.

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

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

[36] 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.

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

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

[39] 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).

appearing to Ofcom to have the skills necessary to prepare a report about matters relevant to those purposes.[40]

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[41] or to the development or sourcing of technology.[42] 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.[43]

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;[44]

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;[45]

g) the systems and processes used by the service which are designed to identify and remove relevant content;[46] 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:

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;[47] and

---

[40] Sections 122 and 104(3), (4) and (6)(a) of the Act.
[41] Section 123(2) of the Act.
[42] Section 123(3) of the Act.
[43] Section 123(2)(f) and (g) and (3)(f) and (g) of the Act.
[44] 'Functionality' is defined in section 233 of the Act.
[45] See section 234 of the Act for the meaning of 'harm'.
[46] 'Systems and/or processes' refers to human or automated systems and/or processes, including technologies (section 236(1) of the Act).
[47] '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).

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,[48] 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;[49] and

b) the period within which the requirements imposed by the Notice will have effect.[50] This may be for up to 36 months from the last day of the period for compliance (set out at a) above).[51]

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.[52] 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.[53]

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 the Notice is required to be taken.[54] A Technology Notice must contain information about when Ofcom intends to review the Notice.

[48] See section 19 of the Act for the meaning of 'journalistic content'.
[49] Section 125(6)(e) of the Act.
[50] Section 125(6)(f) of the Act.
[51] Section 125(7) of the Act.
[52] Section 125(8)(d) of the Act.
[53] Section 125(9) of the Act.
[54] Section 126(4) of the Act.

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 Technology Notice functions and keep it under review. We must have regard to the guidance when exercising, or deciding whether to exercise, those functions.[55] 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.[56]

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.[57] 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.

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.[58] In our work to secure this objective, we must have regard to the

[55] Section 127 of the Act.
[56] Section 128 of the Act.
[57] See section 3(3) of the Communications Act.
[58] Section 3(2)(g) of the Communications Act.

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 desirability of encouraging investment and innovation in relevant markets, the potential impacts on the needs and interests of specific groups of persons identified, such as the vulnerability of children vulnerability of children, 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').[59] 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.[60]

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 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

[59] 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.
[60] On 2 July 2025, the Secretary of State designated its SSP for Online Safety ('the 2025 SSP'). As of the date of this statement, we have a duty to have regard to the 2025 SSP in carrying out our online safety functions. This is available at: Statement of Strategic Priorities for Online Safety - GOV.UK.

crime and disorder, public safety and the protection of health and morals, and the protection of the rights and freedoms of others.[61] 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.

[61] 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 final advice to the Secretary of State outlined in Section 3 of the Technology Notices Advice Statement.

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 give advice to the Secretary of State on minimum standards of accuracy – we are required by the Act to do so.

A2.4 We do however have discretion in formulating our advice to the Secretary of State on minimum standards of accuracy. This impact assessment will therefore assess the likely impact from our recommendations on how to set minimum standards of accuracy as set out in the Technology Notices Advice Statement. The detailed rationale for our advice is set out in the Technology Notices Advice Statement and is not repeated here.

A2.5 In the context of our impact assessment, we have also considered the potential impacts of our recommendations on economic growth and, in terms of the 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/or 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 we have recommended in this advice; what technology, if any, is ultimately accredited against those standards; and to which services, if any, 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 advice in the Technology Notices Advice Statement.[62]

Stakeholder feedback on our impact assessment

A2.8 We received feedback from one stakeholder that they were pleased to note that our impact assessment stated that Ofcom would reserve the right to not consider a technology where it is found by the court or a competent authority such as the ICO to have been developed in breach of UK data protection requirements. However, they suggested that this should be set out more prominently in the final version of the accreditation documents to avoid it being overlooked.[63]

A2.9 We welcome the stakeholder's feedback about our impact assessment and note that we have restated this below (see paragraph A2.23(b)). This is also reflected in Annex 8, in which we have set out an illustrative example of an accreditation application which applicants might be expected to complete before being considered for accreditation (see paragraph A8.5 and the 'Privacy and Legal Considerations' information category).

A2.10 Whilst no other explicit comments were made about our provisional impact assessment, we recognise that a large number of the comments provided by respondents were about the impacts in general of our proposed advice 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 (albeit reflecting that we are not recommending the inclusion of IPT in the minimum standards of accuracy).

Impact on Part 3 regulated services

A2.11 We do not anticipate that the advice set out in Technology Notices Advice Statement should have any direct impacts on the providers of Part 3 services, including on small and micro businesses. Accreditation of technology against the minimum standards of accuracy on which we are advising would not necessarily mean that any regulated service providers are required to use that technology (nor even that we are recommending its use by those providers).

A2.12 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,

[62] 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.
[63] ICO response to December 2024 consultation, p.8.

as well as give them an opportunity to make representations. As recognised in our Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023, 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. We are not providing advice in this document on the circumstances in which it would be necessary and proportionate to issue a Notice to a particular provider.

A2.13 When considering issuing Technology Notices, 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 on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023.

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

A2.14 Many of the potential impacts to the market of safety technology providers—including costs and competition—arise at the point of accreditation (and re-accreditation) or at the point of issuing a Technology Notice, and so have not been considered in detail when assessing the impact of the advice itself. However, we expect our Technology Notice functions to promote competition and growth, and encourage investment and innovation in trust and safety technology.

A2.15 We have not considered in detail the costs of our recommended approach to setting minimum standards and the associated accreditation process for technology providers, as accreditation is optional. We are not able to compel technology providers to undertake this process.

A2.16 While some stakeholders noted the costs associated with accreditation,[64] with several others suggesting that an overly complex process risks increasing costs,[65] only the Marie Collins Foundation questioned whether our proposal was "unduly arduous".[66] We expect that for companies that have followed good software, model development and documentation practices, the process should not be unduly onerous. We have also aimed to avoid undue cost or complexity where possible, for example, by not recommending independent performance testing as part of the accreditation scheme.

A2.17 We have also developed our recommendations regarding minimum standards of accuracy with a view to providing flexible and future-proof standards which should be applicable to the vast range of technologies potentially in scope of this power. Numerous stakeholders highlighted the importance of such flexibility to our approach.[67] In finalising the standards, we have also been mindful of important considerations highlighted by stakeholders. For

[64] Google response to December 2024 consultation, p.12; IWF response to December 2024 consultation, p.5, p.10.
[65] Cyacomb response to December 2024 consultation, p.14; [✂]; NSPCC response to December 2024 consultation, pp.2-3; Ukie response to December 2024 consultation, p.2, pp.6-7, pp.8-10; Videntifier response to December 2024 consultation, p.2.
[66] Marie Collins Foundation response to December 2024 consultation, p.4
[67] CELCIS response to December 2024 consultation, p.1; Cyacomb response to December 2024 consultation, p.1; Google response to December 2024 consultation, p.3; IWF response to December 2024 consultation, p.4; [✂]; NSPCC response to December 2024 consultation, p.1; [✂]; Ukie response to December 2024 consultation, p.2, p.3, p.6.

example, Cyacomb noted that some technologies Ofcom may want to consider (and accredit) might not have been deployed at scale yet.[68] We have therefore modified some of the Objectives and illustrative questions to provide greater flexibility and to incorporate such feedback where appropriate – for more information on responses to stakeholder feedback, please refer to Annex 7. The proposals should also be clear and understandable to those seeking accreditation of their technologies, including small and micro businesses.

Impact on safety outcomes for users of Part 3 services

A2.18 We do not anticipate that the advice set out in the Technology Notices Advice Statement should have any direct impacts on the users of Part 3 services. As noted above, accreditation of technology against the minimum standards of accuracy on which we are advising would not mean that the providers of any Part 3 services are required to use that technology (nor even that we are recommending its use by those providers).

A2.19 We are also not providing advice in the Advice Statement on the circumstances in which it would be necessary and proportionate to issue a Notice to a particular provider. Any decision on whether it is necessary and proportionate 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.

A2.20 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 the advice set out in the Advice Statement. Further, we have taken this into account in our recommendations by seeking to ensure that minimum standards of accuracy are no higher than is necessary (including by not recommending the inclusion of IPT as part of the minimum standards of accuracy), and by making them principles-based.

A2.21 Further, while a risk nevertheless remains that no technologies are able to meet the standards on which we are advising, we consider this would likely indicate that no applicants had sufficiently accurate technology. The fact that Ofcom would not be able to require the use of technology in a Technology Notice in that case would be in line with the Act.

Impact on rights

A2.22 As explained from 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. This is a point that was emphasised by a number of respondents to our December 2024 consultation.

A2.23 While accreditation of such technologies would not mean that the providers of any Part 3 services are required to use them, we have considered the way in which our advice on minimum standards of accuracy could impact these rights:

a) First, our recommendations relating to minimum standards of accuracy have been designed to ensure that the technology developer has taken steps to assure the accuracy of the technology, and as a result to help limit impacts on rights to freedom of expression from accredited technologies. We are recommending that the ABA include a

[68] Cyacomb response to December 2024 consultation, pp.3-4.

range of Objectives relevant to a technology's accuracy in a broad sense. Rather than relying solely on technical performance, our advice recognises that an assessment of accuracy should be sufficiently flexible to include a broad range of socio-technical factors which could potentially impact a technology's accuracy (and thereby users' rights). We have also modified our advice in response to stakeholder feedback to our December 2024 consultation with users' rights impacts in mind. For example, we have recommended that all Objectives be made 'no fail', and that Objective 1.1: Performance Metrics require a higher score (80/100) than other Objectives, and evidence of comprehensive testing against the false positive rate metric (and other appropriate metrics).

b) Second, our proposals relating to minimum standards of accuracy have also been designed with users' rights to privacy in mind. One of the Objectives in the audit-based assessment, for example, is that the technology has been developed with sufficient cybersecurity, privacy and data protection measures in place. We have also explained in paragraph A7.27 in Annex 7 that Ofcom, or a nominated third party, would reserve the right to not consider a technology against the minimum standards of accuracy. This would be where it is found by a Court or other competent authority (such as the ICO) to have been developed in breach of UK data protection or other legal requirements.

A7.22 We note that, while not part of our advice on minimum standards of accuracy, our Technology Notice Guidance explains that Ofcom will have careful regard to rights impacts, taking account of all the available evidence and 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.

Equality legislation and Welsh language

A2.24 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.

A2.25 The relevant protected characteristics are age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

A2.26 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.

A2.27 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.[69] Accordingly, we have considered:

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

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

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

Equality Impact Assessment

A2.28 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 final advice, which has been formulated taking into account the stakeholder feedback we received and further evidence we have gathered, and our assessment of the impact remains unchanged.

A2.29 We have given careful consideration to whether our final advice 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.

A2.30 When thinking about equality, we also think more broadly than persons who share protected characteristics identified in equalities legislation and consider potential impacts on other groups of persons who may be impacted by our proposals.

A2.31 We do not consider our final advice will have any adverse impacts on equality, as we are not requiring the use of any technologies as part of this advice.

[69] The Welsh Language Standards with which Ofcom is required to comply are available on our website.

A2.32 Further, Fairness is one of the assessment Principles we have included within our final advice regarding minimum standards of accuracy. To this extent, our final advice should further equality, including the interests of those with protected characteristics.

A2.33 We also 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. This is reflected in paragraph 3.9(c) of our Guidance.

Welsh Language Impact Assessment

A2.34 We received no specific feedback relating to the Welsh language impact assessment included in our December 2024 consultation on our policy proposals for minimum standards of accuracy. Nonetheless, we have considered the impact of our final advice, which has been formulated taking into account the stakeholder feedback we received and further evidence we have gathered, and our assessment of the impact remains unchanged.

A2.35 In particular, we do not consider our advice 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 final advice differently so as to have a positive impact on the Welsh language, for example, by including accuracy in the Welsh language as a specific standard within the minimum standards of accuracy.

A2.36 However, we note that 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.

A3. Glossary

A3.1 This glossary defines the terms and metrics (in alphabetical order) that we have used throughout this Advice 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.
Adversarial attack	Involves manipulating input data to deceive the technology in making incorrect outputs, predictions, or classifications. For example, evasion attacks, injection attacks, and input perturbations.
Benign (content or data)	In the context of this advice, benign data is information that is not categorised as terrorism or CSEA content. It may still include data or content that is otherwise categorised as harmful.
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.
Confidence scores	Represent the uncertainty of a technology about its predictions and/or classifications.
Confidence thresholds	Refers to the minimum accepted confidence scores.
Confusion matrix	Used to evaluate the predictive performance of a classification technology by breaking down the predictions into true positive, true negative, false positive, and false negative. Key performance metrics such as accuracy, precision, and recall can then be calculated from the confusion matrix.

Term	Definition
Collision rate	Refers to the probability of two distinct inputs producing the same hash value as an output from a hash function.
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.
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.
CSEA content	Refers to content that amounts to an offence specified in Schedule 6 to the Act.
Data labelling	Data labelling is the process of identifying raw data (such as, images, text, videos, etc.) and adding one or more meaningful and informative labels to provide context. References to data labelling, labels and labelling data should be construed accordingly.
Deployment	For the purpose of this advice, this refers to an operational technology being put into use on a particular internet service. References to deploy shall be construed accordingly.
Development data	Data used to develop or train a technology. This might contain training data, datasets, databases, hashes, etc.

Term	Definition
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.
Explainability	Involves post-hoc methods used to analyse how a machine learning-based technology produces its outputs. These explanations are generated after training and can take various forms, such as visualisations, feature importance plots, or textual explanations.
F1 Score	A metric that combines precision and recall into a single score to reflect how well a technology balances correctly predicting positive cases and identifying most of the actual positive cases, calculated as two times the product of precision and recall divided by the sum of precision and recall.
False Negative (FN)	Incorrectly classifying a positive sample as negative.
False Negative Rate (FNR)	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 (FP)	Incorrectly classifying a negative sample as positive.
False Positive Rate (FPR)	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).
Hash	For the purposes of this advice, 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.
Independent evaluation	An unbiased assessment of the technology conducted by a party with no direct involvement with the technology.
Independent verification	The process of checking the correctness and consistency of the approach taken, this might involve checking if the analysis has been technically carried out in a sound manner.
Independent validation	The process of checking whether the approach taken meets the requirements, this might address the question of whether the analysis that has been carried out is sufficient or extensive enough.
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).
Interpretability	Refers to when the behaviours and decisions made by a technology can be easily understood by humans. A technology is interpretable when its structure or operation is inherently understandable, or sufficient documentation makes its structure or operation clear.
Keyword matching/detection	This is a type of technology which can be used as a content moderation tool, including to detect illegal content. Broadly speaking, it can involve a process of matching words and/or phrases to words and/or phrases previously identified as indicative of a particular harm or offence.
Metadata	For the purpose of this advice, 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.
Part 3 service	Refers to a regulated user-to-user service or a regulated search service.

Term	Definition
Precision	The proportion of positive predictions made by a technology that are actually correct, calculated by dividing the number of true positives by the total number of predicted positive cases (true positives and false positives).
Priority illegal content	Content which amounts to a priority offence.
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.
Recall / True Positive Rate (TPR)	The proportion of actual positive cases correctly identified by a technology, calculated by dividing the number of true positives by the total number of actual positive cases (true positives and false negatives)
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 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 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.
Receiver Operating Characteristic (ROC) Curve	A graphical plot of true positive rate versus false positive rate for different classification thresholds in binary classification.
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.
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.

Term	Definition
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.
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.
Terrorism content	Content that amounts to 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.
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.
Testing datasets	Unseen datasets used to evaluate the performance of the technology, which were not present in the development data.
Throughput	A measure of how many pieces of content a technology can process per unit of time, often reported as 'requests per second', and computed by dividing the total number of pieces of content processed in a given timeframe by the length of the timeframe in seconds.
True Negative (TN)	Correctly classifying a negative sample as negative.
True Negative Rate	The proportion of negative cases correctly predicted by a technology. In other words, the technology predicts that the example is negative, and it is actually negative.

Term	Definition
True Positive (TP)	Correctly classifying a positive sample as positive.
URL (Uniform Resource Locator)	A reference that specifies the location of a resource accessible by means of the internet.
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.
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.