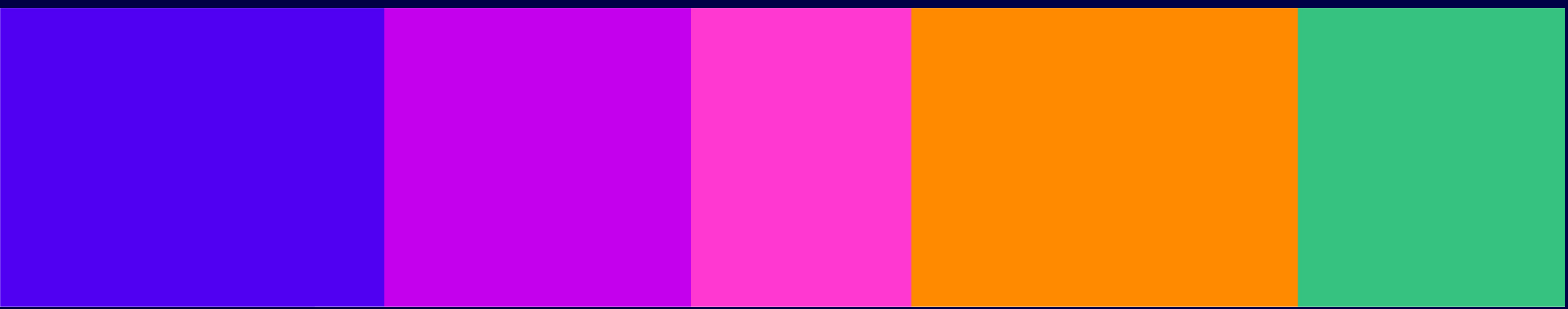


# Annual Report on Notices to deal with terrorism content and/or CSEA content

---

For the year ending 31 December 2024





**Office of Communications**

**Annual Report on Notices to  
deal with terrorism content  
and/or CSEA content**

**For the year ending 31 December 2024**

Presented to Parliament pursuant to section 128(2) of the Online Safety Act  
2023.

23 January 2025



© Ofcom copyright 2025

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](https://nationalarchives.gov.uk/doc/open-government-licence/version/3).

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at [www.gov.uk/official-documents](http://www.gov.uk/official-documents).

Any enquiries regarding this publication should be sent to us at [technologynotices@ofcom.org.uk](mailto:technologynotices@ofcom.org.uk).

ISBN 978-1-5286-5402-9

E03280619 01/25

Printed on paper containing 40% recycled fibre content minimum.

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

# Contents

---

## Section

1. Overview .....	4
2. Background.....	5
3. Year 1 report.....	9

# 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. Part 7 of the Act sets out Ofcom's powers and duties in relation to regulated services. These include a specific power under Chapter 5 of Part 7 of the Act, where we consider it necessary and proportionate, to issue 'notices to deal' with two specific types of illegal content; terrorism and/ or CSEA content.
- 1.2 This document is Ofcom's annual report pursuant to section 128 of the Act in respect of the calendar year 2024. It is a report about:
  - a) the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Act during that period (our 'Technology Notice functions'), and
  - b) technology which meets, or is in the process of development so as to meet, minimum standards of accuracy for the purposes of that chapter.
- 1.3 This report has been sent to the Secretary of State, who has laid it before Parliament.

## Summary of the report

This is Ofcom's annual report for 2024, and is our first annual report under section 128 of the Act since the relevant provisions came into force on 10 January 2024. However, we have undertaken preparatory work in advance of 2024, and therefore we also include references to work undertaken in 2023.

In this report we explain how Ofcom has laid the groundwork for the use of our Technology Notice functions. This has led to the publication of our consultation setting out proposals for our advice to the Secretary of State on minimum standards of accuracy and our draft guidance for the providers of Part 3 services on how we propose to exercise our Technology Notice functions. Currently, this part of the regime is not active and the Secretary of State cannot approve or publish any minimum standards of accuracy until they have received advice from Ofcom.

# 2. Background

## Introduction

---

- 2.1 The Act provides that terrorism content and Child Sexual Exploitation and Abuse ('CSEA') content are both categories of priority illegal content, and Ofcom has been given a range of duties and powers to address such content. These include the power to issue Codes of Practice setting out recommended measures that regulated services can take to comply with their online safety duties (including in respect of terrorism and CSEA content), and to take enforcement action when they are not in compliance.
- 2.2 In addition, Chapter 5 of Part 7 of the Act gives Ofcom the power to issue a 'Technology Notice' requiring a provider of a Part 3 service to deal with terrorism and/or CSEA content when we consider it necessary and proportionate to do so.
- 2.3 This Section provides an overview of the legal framework relating to our power to issue a Technology Notice, including what terrorism and CSEA content are, what Ofcom can require in a Technology Notice and the safeguards that are in place before Ofcom can issue a Notice.

## Legal framework

---

### What is terrorism and CSEA content?

- 2.4 Terrorism and CSEA content are both categories of 'priority illegal content' under the Act.
- 2.5 'Illegal content' is a new concept created by the Act, defined as 'content that amounts to a relevant offence'.<sup>1</sup> 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.<sup>2</sup> '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.<sup>3</sup>
- 2.6 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.

---

<sup>1</sup> Content may consist of 'certain words, images, speech or sounds'. A full definition of illegal content may be found in section 59 of the Act.

<sup>2</sup> 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.

<sup>3</sup> 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.

- 2.7 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) of 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.
- 2.8 Terrorism content refers to content which amounts to an offence specified in Schedule 5 of 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.
- 2.9 CSEA content refers to content which amounts to an offence specified in Schedule 6 of 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.

## What can Ofcom require in a Technology Notice?

- 2.10 Ofcom may issue a Technology Notice to the provider of a Part 3 service,<sup>4</sup> that is, a regulated user-to-user service or regulated search service (or a combined service) (a 'service'),<sup>5</sup> to:
- a) use accredited technology to deal with terrorism and/or CSEA content; or
  - b) use best endeavours to develop or source technology which meets minimum standards of accuracy to deal with CSEA content.
- 2.11 For a Technology Notice requiring the use of accredited technology:
- a) user-to-user services may be required to use that technology to identify and swiftly take down, or prevent individuals from encountering, terrorism content or CSEA content; and

---

<sup>4</sup> See section 121 of the Act.

<sup>5</sup> 'User-to-user services' and 'search services' are defined in section 3 of the Act. These services will be regulated for the purposes of the Act if the service has links with the UK and does not fall within Schedule 1 or Schedule 2 of the Act (see section 4 of the Act). A 'combined service' means a regulated user-to-user service that includes a public search engine – see section 4(7) of the Act.

- b) search services may be required to use that technology to identify search content of the service that is terrorism or CSEA content and swiftly take measures to secure that, so far as possible, search content no longer includes such content identified by the technology.
- 2.12 For a Technology Notice requiring the sourcing or development of technology, services may be required to use best endeavours to develop or source technology, which meets minimum standards of accuracy, that can be used:
- a) in the case of user-to-user services, to identify and swiftly take down, or prevent individuals encountering, CSEA content; and
  - b) in the case of 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.
- 2.13 For 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; and accredited technology to address terrorism content communicated publicly by means of the service. The Act specifies factors that we must particularly consider when deciding whether content is communicated ‘publicly’ or ‘privately’ for the purposes of a Technology Notice.<sup>6</sup>

## What does ‘accredited technology’ mean?

- 2.14 Technology is ‘accredited’ if it is accredited by Ofcom, or another person appointed by Ofcom, as meeting minimum standards of accuracy in the detection of terrorism and/or CSEA content.<sup>7</sup> Those minimum standards of accuracy must be such standards as are for the time being approved and published by the Secretary of State, following advice from Ofcom.<sup>8</sup> Where a Technology Notice requires a Part 3 service provider to use best endeavours to develop or source technology to deal with CSEA content this requires them to aim to develop or source technology which meets those minimum standards.

## Considerations for Ofcom before issuing a Technology Notice

- 2.15 Before Ofcom can exercise its Technology Notice functions, some important steps need to have been taken:
- a) Ofcom must advise the Secretary of State about minimum standards of accuracy in the detection of terrorism content and CSEA content before the Secretary of State can approve and publish them.
  - b) Before it can issue a Notice requiring the use of a specific technology, Ofcom or a nominated third party must have **accredited that technology** against the minimum standards of accuracy; and
  - c) Ofcom must **produce guidance for Part 3 service providers** about how it proposes to exercise its Technology Notice functions.

---

<sup>6</sup> See section 232 of the Act. These are: 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. See Ofcom, [Guidance on content communicated ‘publicly’ and ‘privately’ under the Online Safety Act](#) [accessed 17 December 2024].

<sup>7</sup> Section 125(12) of the Act.

<sup>8</sup> Section 125(13) of the Act. See also paragraph 3.2 below.

- 2.16 There are several additional steps and/or safeguards within the Act before Ofcom will be able to issue a Technology Notice to a particular provider of a Part 3 service. Specifically, Ofcom must:
- a) **obtain a report from a skilled person** to assist us in deciding whether to give a Technology Notice, and to advise about the requirements that might be imposed;
  - b) give a **warning notice** to the provider of a Part 3 service, which outlines the requirements that Ofcom is considering imposing in a Technology Notice, and provide them with the opportunity to make representations on it; and
  - c) be satisfied that it is **necessary and proportionate** to issue a Technology Notice. In determining whether it is necessary and proportionate in a particular case, Ofcom is required to consider a range of matters, including (but not limited to) the kind of service; the prevalence of, and extent of dissemination of, terrorism or CSEA content on the service; and the systems and processes already used by the service to identify and remove terrorism/CSEA content.<sup>9</sup>
- 2.17 When requiring the use of a specific technology (rather than best endeavours to develop or source technology), Ofcom is also required to consider matters such as the extent to which use of the specified technology might result in interference with users' right to freedom of expression,<sup>10</sup> and the level of risk of the use of that technology breaching privacy (including data protection) requirements.<sup>11</sup>

---

<sup>9</sup> Section 124 of the Act specifies the matters we must consider, in particular, when making our decision.

<sup>10</sup> Section 124(2)(i) of the Act.

<sup>11</sup> Section 124(2)(j) of the Act.

# 3. Year 1 report

## The exercise of our Technology Notice functions

---

- 3.1 As noted at paragraph 2.15, before Ofcom can exercise its Technology Notice functions, there are important steps that need to be taken. At present, this part of the regime is not active and the Secretary of State cannot approve or publish any minimum standards of accuracy until they have received advice from Ofcom. Therefore, we have not yet been in a position to assess whether or not there is any technology which meets, or is in the process of development to meet, any such minimum standards of accuracy.
- 3.2 However, we have undertaken a significant amount of preparatory work over the last year (and in 2023) in relation to our Technology Notice functions. This culminated in the recent publication of our [Consultation on policy proposals for minimum standards of accuracy for accredited technologies, and guidance to providers](#) ('Consultation: Technology Notices')<sup>12</sup> in which we are consulting on our policy proposals for our advice to the Secretary of State on setting minimum standards of accuracy, and our draft guidance for the providers of Part 3 services on the exercise of our Technology Notice functions. This was published on **16 December 2024**.
- 3.3 The work we have undertaken to inform our consultation, and our work more generally in relation to this power, includes:
- i) **Information Requests:** in early 2024 we issued statutory information requests to ten companies that have developed terrorism and/or CSEA content detection technology, including several providers of Part 3 regulated services. From the responses, we learnt how the technology developers conceptualise and assess the performance of their technologies, particularly before deployment or making them available to third parties.
  - ii) **Multi-stakeholder workshop:** in October 2023, we invited 30 organisations to a workshop coordinated by a market research and consulting company, Ipsos, at Ofcom's London office. The workshop helped us understand stakeholders' views on minimum standards of accuracy, the accreditation process and the Technology Notice power more generally.<sup>13</sup>
  - iii) **External research:** we commissioned an external consultancy, PUBLIC, in May 2023, to help us better understand how to develop an accreditation scheme. PUBLIC's research looked at how existing accreditation processes have been developed, evaluated and operationalised from 11 accreditation approaches across five sectors.<sup>14</sup>

---

<sup>12</sup> Ofcom, [Consultation: Technology Notices](#) [accessed 17 December 2024].

<sup>13</sup> Ipsos, [Ipsos Multi-Stakeholder Workshop Report](#) [accessed 17 December 2024].

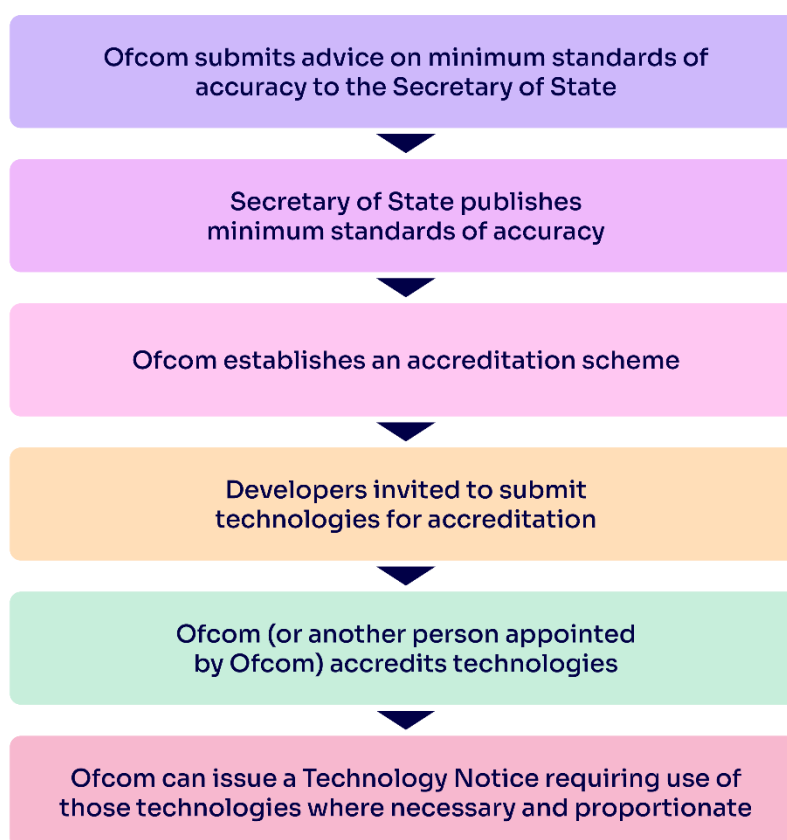
<sup>14</sup> Ofcom, [PUBLIC Tech Accreditation Landscape Report](#) [accessed 17 December 2024].

## Our next steps

---

- 3.4 We are inviting stakeholders' views on our [Consultation: Technology Notices](#) published in December. The deadline for responses is **5pm on Monday 10 March 2025**.<sup>15</sup>
- 3.5 During 2025 we also plan to undertake further work to determine how the accreditation scheme will work, which may include commissioning further external research. Taking account of this work and subject to consultation responses, we will then issue our advice on minimum standards of accuracy to the Secretary of State. We expect to publish our final guidance for providers of Part 3 services on the exercise of our Technology Notice functions at the same time as our advice to the Secretary of State.

Figure 1- A summary of the steps required before Ofcom can issue a Technology Notice



---

<sup>15</sup> Ofcom, [Consultation: Technology Notices](#) [accessed 17 December 2024].







E03280619

978-1-5286-5402-9