EXPLANATORY NOTES

Online Safety Act 2023

Chapter 50

£28.14

tso
a Williams Lea company

Published by TSO (The Stationery Office), a Williams Lea company, and available from:

Online
www.tsoshop.co.uk

Mail, Telephone & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0333 202 5070
E-mail: customer.services@tso.co.uk
Textphone: 0333 202 5077

ISBN 978-0-10-560365-8

9 780105 603658

ONLINE SAFETY ACT 2023

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Online Safety Act 2023 which received Royal Assent on 26 October 2023 (c. 50).

- These Explanatory Notes have been prepared by the Department for Science, Innovation and Technology in order to assist the reader in understanding the Act. They do not form part of the Act and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Act will mean in practice; provide background information on the development of policy; and provide additional information on how the Act will affect existing legislation in this area.
- These Explanatory Notes might best be read alongside the Act. They are not, and are not intended to be, a comprehensive description of the Act.

Table of Contents

These Explanatory Notes relate to the Online Safety Act 2023 which received Royal Assent on 26 October 2023 (c. 50).

These Explanatory Notes relate to the Online Safety Act 2023 which received Royal Assent on 26 October 2023 (c. 50).

These Explanatory Notes relate to the Online Safety Act 2023 which received Royal Assent on 26 October 2023 (c. 50).

These Explanatory Notes relate to the Online Safety Act 2023 which received Royal Assent on 26 October 2023 (c. 50).

These Explanatory Notes relate to the Online Safety Act 2023 which received Royal Assent on 26 October 2023 (c. 50).

These Explanatory Notes relate to the Online Safety Act 2023 which received Royal Assent on 26 October 2023 (c. 50).

Overview of the Act

1 The Online Safety Act establishes a new regulatory regime to address illegal and harmful content online. It imposes legal requirements on:

- Providers of internet services which allow users to encounter content generated, uploaded or shared by other users ("user-to-user services");
- Providers of search engines which enable users to search multiple websites and databases ("search services"); and
- Providers of internet services on which provider pornographic content (pornographic content that is published by a provider and is not user-generated) is published or displayed.

2 The Act confers new powers on the Office of Communications (OFCOM) establishing them as the online safety regulator. This role includes overseeing and enforcing the new regulatory regime.

Policy background

3 As use of the internet has expanded, there is growing public concern about the prevalence and spread of illegal online content, as well as the risks to children's safety arising from exposure to inappropriate content, such as pornography.

4 Research and public polling has also highlighted users' concerns about how platforms are applying their own terms and conditions, and how they respond to users' complaints.

Existing Regulation of Online Services

5 Prior to the enactment of this Act, most user-to-user and search services operating in the United Kingdom were not subject to any regulation concerning user safety for user generated content.

6 A limited number of user-to-user services which are used in the United Kingdom are subject to the Video Sharing Platform regime set out in Part 4B of the Communications Act 2003 (the "VSP Regime"). Only services which meet the legal definition of a video sharing platform[1] and have the required connection with the United Kingdom[2] are in scope.

[1] The legal test is set out in Section 368S of the Communications Act 2003. OFCOM have produced guidance on the definition of a video sharing platform which is available on the OFCOM website.

[2] Sections 368S(3)-(5) of the Communications Act 2003 sets out when a video sharing platform will be regarded as having the required connection with the United Kingdom for the purposes of the VSP Regime. OFCOM have produced guidance in relation to when a video sharing platform will be regarded as established in the United Kingdom, which is available on the OFCOM website.

7 Services subject to the VSP Regime are required to take measures to:

a. Protect the public from videos and adverts likely to incite violence or hatred against a person on specified grounds including sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political opinion, membership of a national minority, disability, age and sexual orientation;

b. Protect the public from material in videos or adverts where the inclusion of that material would be a criminal offence under laws relating to terrorism, child sexual abuse material, and racism and xenophobia;

c. Protect under 18s from videos and adverts which have or would be likely to be given an R18 certificate,[3] or which have been or would likely be refused a certificate by the British Board of Film Classification;[4] and

d. Protect under 18s from videos and adverts containing material that might impair their physical, mental or moral development.

8 The VSP Regime does not set standards for the content of individual videos.

9 OFCOM are responsible for enforcing video sharing platform providers' compliance with their obligations under the VSP Regime. OFCOM have the power to give enforcement notifications (which may set out the steps required to remedy a contravention)[5] and to impose financial penalties of up to £250,000 or 5% of qualifying revenue, whichever is greater.[6] In certain circumstances, OFCOM may also suspend and/or restrict a service.[7]

The Online Harms White Paper

10 The Online Harms White Paper, published in April 2019, set out the Government's intention to introduce a new regulatory framework to improve protections for users online. It was proposed that this objective would be achieved via a new duty of care on companies, and an independent regulator responsible for overseeing the online safety framework. The White Paper proposed that the regulatory framework should follow a proportionate and risk-based approach, and that the duty of care should be designed to ensure that all in-scope companies had appropriate systems and processes in place to address harmful content and improve the safety of their users.

---

[3] The R18 category is a special and legally-restricted classification, primarily for explicit videos of consenting sex or strong fetish material involving adults, and where the primary purpose of the material is sexual arousal or stimulation.

[4] The BBFC's current guidelines outline that material likely to be unsuitable for classification could include: material which is in breach of criminal law (or created through the commission of a criminal offence); material that appears to risk harm to individuals or to society such as, for example, the detailed portrayal of violence or dangerous acts, illegal drug use; and the portrayal or invitations to conduct sadistic violence, rape or other non-consensual sexual violent behaviour or other harmful violent activities.

[5] Sections 368Z2 and 368Z3 of the Communications Act 2003.

[6] Section 368Z4 of the Communications Act 2003.

[7] Sections 368Z5 and 368Z6 of the Communications Act 2003.

11 A public consultation on the White Paper proposals ran from 8 April 2019 to 1 July 2019. It received over 2,400 responses ranging from companies in the technology industry (including large tech giants and small and medium sized enterprises), academics, think tanks, children's charities, rights groups, publishers, governmental organisations, and individuals.

12 In February 2020, the Government published an initial response to the consultation, providing an in-depth breakdown of the responses to each of the 18 consultation questions asked in relation to the White Paper proposals. The response also set out the Government's direction of travel in a number of key areas, including:

a. How the new regulatory framework would ensure protections for users' rights by including safeguards in the legislation;

b. The differentiated approach to illegal and legal but harmful material;

c. How the new requirements would be proportionate and risk-based, including clarifying who would not be captured by the proposed scope;

d. A commitment to delivering a higher level of protection for children; and

e. That the Government was minded to appoint OFCOM as the new regulator.

13 In December 2020, the full Government response to the consultation was published, outlining the final policy position for the online safety regulatory framework, and the Government's intention to enshrine it in law through the Online Safety Act. The response was split into seven parts:

a. Part 1 stated that the regulatory framework would apply to companies whose services host user-generated content or facilitate interaction between users, one or more of whom is based in the United Kingdom, as well as to search engines.

b. Part 2 outlined that the legislation would set out a general definition of the harmful content and activity covered by the duty of care. It also set out how all companies in scope would be required to understand the risk of harm to individuals on their services, and to put in place appropriate systems and processes to improve user safety and monitor their effectiveness.

c. Part 3 confirmed that OFCOM would be appointed as the regulator, and outlined their regulatory functions and funding.

d. Part 4 explained the proposed functions of the regulator, including their duty to set out codes of practice, enforcement powers, and user redress mechanisms.

e. Part 5 outlined the role of technology, education, and awareness in tackling online harms.

f. Part 6 explained how the new regulatory framework would fit into the wider digital landscape, including as part of the Government's Digital Strategy.

g. Part 7 provided the next steps for the regime, including the expected timings for the Online Safety Act.

Interim Codes of Practice

14 The Government published two interim codes of practice covering terrorist content and child sexual exploitation and abuse (CSEA) content online alongside the full government response. These interim codes set out the voluntary action the Government expects providers to take to tackle the most serious categories of harmful content online before OFCOM issues codes of practice using the powers conferred by the Act.

Government Report on Transparency Reporting

15 The first government report on transparency reporting in relation to online harms was published alongside the full government response. This presented the recommendations of the multi-stakeholder transparency working group, set up in October 2019, about how the transparency framework could work in practice within the new online harms regulatory framework.

Pre-legislative Scrutiny

16 In May 2021 the Online Safety Bill was published in draft. A Joint Committee of MPs and Peers, chaired by Damian Collins MP, was established on 23 July 2021 to carry out pre-legislative scrutiny. The Joint Committee took evidence from over 50 witnesses and received over 200 pieces of written evidence. The Committee published its report and recommendations on 10 December 2021.

17 The Government responded to the report on 17 March 2022 confirming that a number of substantive changes were made to the Act at introduction, including, but not limited to:

a. Including priority offences in primary, rather than secondary legislation;

b. Including a new standalone provision for non-user-generated pornography, meaning all providers of online pornography are in scope of the legislation;

c. Including the Law Commission's recommendations for new online communications offences;

d. Amending the senior manager liability offence so that it would be commenced three months after Royal Assent;

e. Including a new duty on Category 1[8] providers to offer optional user verification and user empowerment tools on their sites;

f. Including a new duty on Category 1 and Category 2A providers to protect users from fraudulent advertising online; and

g. Simplifying the definition of non-designated harmful content, and requiring Category 1 providers only to address categories of content that are legal but harmful to adults, which are designated in secondary legislation.

[8] Category 1 services is a subset of user-to-user services that is subject to additional duties.

The Online Safety Act

18 The legislation imposes legal requirements on:

a. Providers of internet services which allow users to encounter content generated, uploaded or shared by other users, i.e. user-generated content ("user-to-user services");

b. Providers of search engines which enable users to search multiple websites and databases ("search services"); and

c. Providers of internet services on which provider pornographic content is published or displayed.

19 The legislation requires providers of regulated user-to-user and search services to:

a. Assess the risks of harm to those users present on the service;

b. Take steps to mitigate and manage the risks of harm to individuals arising from illegal content and activity, and (for services likely to be accessed by children) content and activity that is harmful to children. Providers will also need to assess the risk of their services being used for the commission or facilitation of a priority offence and to design and operate their services to mitigate this risk;

c. Put in place systems and processes which allow users and affected persons to report specified types of content and activity to the service provider;

d. Establish a transparent and easy to use complaints procedure which allows for complaints of specified types to be made;

e. Have particular regard to the importance of protecting users' legal rights to freedom of expression and protecting users from a breach of a legal right to privacy when implementing safety policies and procedures; and

f. Put in place systems and processes designed to ensure that detected but unreported CSEA content is reported to the NCA.

20 Those user-to-user services which meet the Category 1 threshold conditions, specified by the Secretary of State, are subject to additional legal requirements, including to:

a. Improve transparency and accountability and protect free speech. Those user-to-user services which meet the Category 1 threshold conditions must have systems and processes to ensure they only remove or restrict access to content, or ban or suspend users, where allowed by their terms of service, or where they otherwise have a legal obligation to do so.

b. Carry out an assessment of the impact that safety policies and procedures will have on users' legal rights to freedom of expression, including on access to and treatment of news publisher and journalistic content, and users' privacy, and demonstrate the steps they have taken to mitigate any impact;

c. Specify in a public statement the steps taken to protect users' legal rights to freedom of expression and users' privacy;

d. Put in place systems and processes designed to ensure that the importance of the free expression of content of democratic importance is taken into account when making decisions about how to treat such content;

e. Put in place systems and processes designed to ensure that the importance of the free expression of journalistic content is taken into account when making decisions about how to treat such content.

f. Notify and offer a right of appeal to a recognised news publisher before removing or moderating its content, or taking action against its account;

g. Put in place a dedicated and expedited complaints procedure that ensures that the decisions of the service provider to take action against a user because of a particular piece of journalistic content can be challenged;

h. Offer optional user verification and user empowerment tools to adults on their sites; and proactively ask their registered adult users at the first possible opportunity how they would like the user empowerment content tools to be applied; and

i. Put in place proportionate systems and processes to prevent the risk of users encountering fraudulent adverts.

21 Those search services which meet the Category 2A threshold conditions are under a duty to produce annual transparency reports and to put in place proportionate systems and processes to prevent the risk of users encountering fraudulent adverts.

22 Category 1, 2A, and 2B Services are also under duties to set out their policies on disclosing information to the parents of deceased child users, provide details about this in the terms of service or a publicly available statement, and operate a complaints procedure in relation to these duties.

23 The Act confers new powers on OFCOM establishing them as the online safety regulator. OFCOM is responsible for enforcing the legal requirements imposed on service providers. The Act gives OFCOM the power to compel in-scope providers to provide information and to require an individual from an in-scope provider to attend an interview; powers of entry and inspection; and the power to require a service provider to undertake, and pay for, a report from a skilled person. OFCOM may also require information, or produce a report, in relation to the death of a child and share this information with a coroner.

24 The Act confers new powers on OFCOM to require regulated user-to-user and search services to use accredited technology to deal with CSEA and terrorism content, or make best endeavours to develop or source technology to deal with CSEA content, where necessary and proportionate.

25 The new powers conferred on OFCOM also include the power to give enforcement notifications (which may set out the steps required to remedy a contravention) and the power to impose financial penalties of up to £18 million or 10% of qualifying worldwide revenue, whichever is greater. OFCOM can also, in certain circumstances, apply to the Courts for an order imposing business disruption measures on a provider.

26 The Act requires OFCOM to produce codes of practice for service providers, setting out the recommended steps that providers can take in order to comply with the legal requirements described above. A provider may take different measures to those recommended in the codes of practice. A provider will be treated as having complied with the relevant legal obligation if the provider takes the steps recommended in the relevant code of practice for complying with that obligation.

27 The Act also requires providers of internet services which make pornographic material available by way of the service (as opposed to enabling users to generate or share such content) to use age verification or age estimation (or both), to ensure that children are not normally able to encounter that pornographic content.

28 The Act creates a false communications offence and a threatening communications offence. It also amends the existing communications offences in the Malicious Communications Act 1988, Malicious Communications (Northern Ireland) Order 1988, and Section 127 of the Communications Act 2003 to reflect this. It also creates a new "cyberflashing" offence, an offence of sending or showing flashing images electronically to people with epilepsy, and an offence of encouraging or assisting serious self-harm. It also inserts new intimate image abuse offences to the Sexual Offences Act 2003.

Legal background

29 Prior to the exit of the United Kingdom exit from the European Union, the legal framework for the regulation of online services was primarily set out in the EU e-Commerce Directive (eCD)[9]. The eCD detailed the rules for online service providers in respect of transparency and information requirements, rules for cooperation between member states, and, most importantly for the purposes of the Act, a framework limiting the liability of online intermediaries for the content they host on their services.

30 The eCD prevented member states from imposing liability on service providers who provide a service that '*consists of the storage of information provided by the recipient of the service*' for content created by users, so long as '*the provider does not have actual knowledge of illegal activity or information and ... is not aware of facts or circumstances from which the illegal activity or information is apparent'*. This limitation was contingent on the host, upon gaining knowledge of such content, removing it expeditiously. Article 15 of the eCD also contained a prohibition on the imposition of requirements on service providers to generally monitor content they transmit or store, or to actively seek facts or circumstances indicating illegal activity.

31 Following the exit of the United Kingdom from the European Union, there is no longer a legal obligation on the United Kingdom to legislate in line with the provisions of the eCD.

32 The Audiovisual Media Services Regulations 2020 transposed the EU's revised Audiovisual Media Services Directive (AVMSD)[10] into United Kingdom law. The AVMSD introduced a new regulatory framework for video sharing platforms. A principal feature of a video sharing platform is that it enables users to upload and share videos with members of the public (with the platform having no editorial control over the content of the video). The Government transposed the VSP framework into Part 4B of the Communications Act 2003, which came into force on 1 November 2021. Further detail on the current regulation of video sharing platforms is set out above.

---

[9] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[10] Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services.

33 Other related legislation includes the Digital Economy Act 2017 ("DEA"). Section 103 of the DEA obliged the Secretary of State to issue a code of practice for providers of online social media platforms setting out guidance on action it might be appropriate for social media providers to take to prevent bullying, insulting, intimidating and humiliating behaviours on their sites. The code of practice was published on 8 April 2019. Part 3 of the DEA put forward a statutory requirement for all commercial pornographic websites to prevent children's access. The Act received Royal Assent in April 2017 but Part 3 was not fully commenced. The government announced in October 2019 that it would not commence Part 3 of the 2017 Act, and would instead repeal Part 3 and deliver its objectives through the online harms regulatory framework. Part 3 is repealed by section 212 of the Online Safety Act.

34 OFCOM are the independent regulator for communications in the United Kingdom. Their remit covers the regulation of broadband and telecoms, TV, radio, video-on-demand services and postal services. They are also responsible for managing the effective use of the radio spectrum.

35 OFCOM were established under the Office of Communications Act 2002. OFCOM are a statutory corporation, and their governance arrangements are set out in the Office of Communications Act 2002. As a public authority, OFCOM are also subject to other legal duties, including requirements to ensure they act in a way that is compatible with human rights (under the Human Rights Act 1998) and comply with data protection legislation.

36 OFCOM's powers are found in the Communications Act 2003 and the Wireless Telegraphy Act 2006, as well as other enactments including the Broadcasting Acts 1990 and 1996, and the Postal Services Act 2011. The Act amends the general duties of OFCOM, as set out in section 3 of the Communications Act 2003, to extend them in relation to online safety matters.

37 The Online Safety Act repeals the following existing legislative provisions which relate to the regulation of internet services:

a. Part 3 of the Digital Economy Act 2017 (online pornography);

b. Section 103 of the Digital Economy Act 2017 (code of practice for providers of online social media platforms); and

c. Part 4B of the Communications Act 2003 (video-sharing platform services), Part 4 of the Audiovisual Media Services Regulations 2020 (S.I. 2020/1062) (which inserts Part 4B into the Communications Act 2003), and Regulation 4 of the Audiovisual Media Services (Amendment) (EU Exit) Regulations 2020.

38 The Online Safety Act repeals the following existing legislative provisions which relate to communications offences:

a. Subsections (2)(a) and (b) of section 127 of the Communications Act 2003 (improper use of electronic communications network), in so far as they extend to England and Wales; and

b. Subsections 1(1)(a)(ii), 1(1)(a)(iii), and 1(2) of the Malicious Communications Act 1988.

c. Section 33 of, and Schedule 8 to, the Criminal Justice and Courts Act 2015.

39 The Online Safety Act repeals the following existing legislative provisions which relate to the sharing or threatening to share intimate photograph or film offences:

a. Sections 33 to 35 of the Criminal Justice and Courts Act 2015 (disclosing or threatening to disclose private sexual photographs and films with intent to cause distress).

b. Section 187: offence of sending etc photograph or film of genitals.

c. Section 188: offences of sharing or threatening to share intimate photograph or film.

Territorial extent and application

40 Section 239 sets out the territorial extent of the Online Safety Act. The extent of an Act can be different from its application. Application is about where an Act produces a practical effect rather than where it forms part of the law. The Online Safety Act extends and applies to the whole of the United Kingdom, aside from the provisions set out below. Further detail is at Annex A.

41 The communications offences under sections 179 to 183 and the repeal in section 189(1) do not extend to Scotland. The provisions set out at section 239(3) extend to England and Wales only. Section 214(4) to (6) extends to Scotland only. Sections 189(3) and 214(7) to (9) extend to Northern Ireland only.

42 The UK Parliament does not normally legislate with regard to matters that are within the legislative competence of the Scottish Parliament, Senedd Cymru or the Northern Ireland Assembly without the consent of the legislature concerned. It is also the practice of the UK Government to seek the consent of the devolved legislatures for provisions which would alter the competence of those legislatures or the devolved administrations in Scotland, Wales and Northern Ireland. The Northern Ireland Assembly was adjourned during the parliamentary passage of the Act.

43 The majority of the Act is outside the competence of the devolved legislatures under the internet services reservation, with the exception of a small number of provisions where the Government sought the consent of the relevant legislatures as follows:

a. The False Communication Offence under sections 179, 180 and 182.

b. The Threatening Communication Offence under sections 181 and 182.

c. The Offence under section 183 of sending or showing flashing images electronically.

d. The Offence under sections 184, 185 and 186 of encouraging or assisting the serious self-harm of another person.

e. The power for Ministers in Scotland, Wales, and the relevant department in Northern Ireland to amend the list of exempt educational institutions included at Part 2 of Schedule 1 under section 221.

f. The power for Ministers in Scotland to amend the list of CSEA offences included in Part 2 of Schedule 6 under section 222(2).

44 In addition, repeals and amendments made by this Act have the same territorial extent as the legislation that they are amending or repealing where specified.

45 See Annex A for a summary of the position regarding territorial extent and application in the United Kingdom.

Extent in the Channel Islands and Isle of Man

46 Section 239 also includes a Permissive Extent Clause, where His Majesty may by Order in Council provide for any of the provisions of this Act to extend, with or without modifications, to the Bailiwick of Guernsey or to the Isle of Man.

Commentary on provisions of Act

47 The Act is divided into 12 parts:

a. **Part 1** contains an introduction section and an overview section, setting out what is included in this Act.

b. **Part 2** contains definitions of the services to which the Act applies.

c. **Part 3** imposes duties of care that apply to providers of regulated user-to-user and search services. It requires OFCOM to issue codes of practice relating to those duties.

d. **Part 4** imposes further duties on providers of regulated user-to-user and search services, including relating to user identity verification, CSEA content, and transparency reporting.

e. **Part 5** imposes duties on providers of regulated services that publish or display provider pornographic content.

f. **Part 6** imposes requirements on providers of regulated services to pay fees.

g. **Part 7** sets out OFCOM's powers and duties.

h. **Part 8** sets out the appeals and complaints procedures relating to regulated services.

i. **Part 9** sets out the Secretary of State's functions in relation to regulated services.

j. **Part 10** sets out new and updated communications offences.

k. **Parts 11 and 12** contain miscellaneous and general provisions. In particular, they define key concepts such as providers of regulated services, users, and internet services.

Part 1: Introduction

Section 1: Introduction

48 This section provides a statement about the general purpose of the new regulatory framework and the main objectives of the duties imposed on in-scope providers. It also makes clear that the Act gives OFCOM new powers and functions as the regulator overseeing the new regulatory framework.

Section 2: Overview of Act

49 This section sets out the subject matters of the various parts of the Act.

Part 2: Key definitions

Section 3: "User-to-user service" and "search service"

50 This section provides definitions for the terms "user-to-user service" and "search service".

51 Subsection (1) defines a user-to-user service as an internet service which allows users to generate, upload or share content which may be encountered by others on that service. Subsection (2) sets out that it does not matter for the purpose of this definition if content is shared with another user on the service as long as the service has a functionality that allows such sharing. It also does not matter what proportion of content on a service is user-generated content.

52 Subsection (4) provides that a search service is an internet service which is, or includes a search engine. "Search engine" is defined in section 229 as a service or functionality which enables a person to search more than one website or database.

53 Subsections (5) to (7) explain whether an internet service that both enables user-generated content and includes a search engine will be a user-to-user service or a search service. If the only user-generated content enabled by the service is of a kind exempted under the relevant provisions of Schedule 1 to the Act, then it will be a search service. If a search service enables other forms of user-generated content, then it will be a user-to-user service.

Section 4: "Regulated service", "Part 3 service" etc

54 This section defines the term "regulated service" and other related terms used in the Act.

55 Subsection (2) sets out when user-to-user services and search services will be regulated user-to-user services and regulated search services. To be regulated, such services must have links with the United Kingdom and not be exempt under Schedule 1 or Schedule 2. Subsection (3) states that these regulated user-to-user services and search services are referred to as Part 3 services in the Act.

56 Subsection (4) defines "regulated service" as meaning a regulated user-to-user service, a regulated search service, or a service with links to the United Kingdom that publishes or displays provider pornographic content.

57 Subsections (5) and (6) clarify the circumstances under which a user-to-user or search service has links with the United Kingdom. A service will be in scope if it has a significant number of users in the United Kingdom or if the United Kingdom is a target market. A service will also be in scope if it can be used in the United Kingdom by individuals and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the United Kingdom. Section 80(4) applies an equivalent test to internet services which publish or display provider pornographic content.

58 As the regulatory framework established by the Act is focused on protecting individuals in the United Kingdom, these provisions ensure that services which do not have links to the United Kingdom are not in scope of regulation.

59 Subsection (7) provides that a regulated user-to-user service that includes a public search engine (i.e. one which is not an internal business service) is referred to in the Act as a "combined service".

Schedule 1: Exempt user-to-user and search services

60 Schedule 1 sets out which user-to-user and search services are exempt from regulatory duties. Subsection (2)(b)(i) of section 4 ("Regulated service'", "Part 3 service" etc) states that services of the descriptions set out in this Schedule are not regulated user-to-user services or regulated search services.

61 Paragraphs 1 to 3 provide that services will be exempt if the only type of user-generated content enabled by the service is, respectively, email, SMS and/or MMS messages (as defined in section 55(12)), or one-to-one live aural communications (as defined in section 55(5)).

62 Under the limited functionality services exemption in paragraph 4, a user-to-user service is exempt if the only ways users can communicate on the service are the following:

a. The posting of comments or reviews on provider content (defined in subparagraph (2) as content published on the service by or on behalf of the service provider).

b. The sharing of those comments or reviews on other internet services.

c. Expressing views on provider content or on comments and reviews on provider content through: (i) a "like" or "dislike" button, (ii) applying an emoji or symbol of any kind, (iii) engaging in yes/no voting or (iv) rating or scoring the provider content or the comments or reviews.

d. Displaying or producing identifying content (e.g. usernames or avatars) in connection with any of these activities.

63 This exempts services where the only user interaction is, for example, 'below the line' content on media articles, or user reviews of directly provided goods and services. Any services that also have additional user-to-user functionalities will remain in regulatory scope.

64 Paragraph 5 sets out that a user-to-user service is also exempt if the only user-generated content it enables is of a kind covered by an exemption listed in paragraphs 1–4 (i.e. emails, SMS/MMS messages, one-to-one live aural communications, or comments and reviews relating to provider content).

65 However, paragraph 6 of Schedule 1 sets out that a service which would otherwise benefit from an exemption set out in the preceding paragraphs is not exempt pornographic content is published or displayed on the service and it has links with the United Kingdom. If paragraph 6 applies to a service, paragraph 1 of Schedule 2 may exempt the service from the user-to-user service duties while keeping it in scope of the Part 5 duties.

66 Paragraph 7 exempts "internal business services". This exemption encompasses services such as business intranets, productivity and collaboration tools, content management systems, customer relationship management systems and database management software. To qualify as an internal business service, the service must meet the conditions set out in paragraph 7(2). Paragraph 8 provides details on the exemptions for internal business services where they make up only part of the user-to-user service or search service.

67 Paragraph 9 provides that some user-to-user and search services provided by certain public bodies are exempt from regulatory duties. This exemption covers services provided by Parliament and foreign governments, as well as services provided by public authorities in the United Kingdom and bodies outside the United Kingdom where those services are provided in the exercise of functions of a public nature only.

68 Paragraph 10 provides an exemption for user-to-user or search services that are provided by education or childcare providers as described in Part 2, where those services are provided for the purpose of education and childcare.

69 Many education and childcare providers are subject to existing safeguarding duties which require them to protect children online. This exemption ensures that those education and childcare providers listed are not subject to oversight by both OFCOM and the relevant oversight bodies for education across the United Kingdom.

70 Paragraph 10(1) specifies a user-to-user service or a search service is exempt if the provider of the service is:

a. The responsible person for that education or childcare for e.g. a governing body of a maintained school in England.

b. A person employed or engaged to provide that education or childcare who is subject to safeguarding duties as defined in sub-paragraph (2), e.g. a teacher employed to work in an independent school in England.

71 Sub-paragraph (3) specifies that the responsible person must be a person who has day-to-day responsibility for the relevant education or childcare provision, for e.g. a governing body, rather than a person who may have a high-level duty to ensure education or child care is provided e.g. a Minister of a government department. A "person" includes (in addition to an individual and a body of persons corporate or unincorporate) any organisation or association of persons.

72 Schedule 1 Part 2 provides a list of descriptions of education and childcare provided in the United Kingdom that is exempt under subsection 10. Any education or childcare providers not described in Part 2 is not exempt under subsection 10.

73 Schedule 1 Part 3 provides a set of definitions for childcare, education, further education, higher education, primary education, and secondary education for each nation in the United Kingdom.

Schedule 2: User-to-user services and search services that include regulated provider pornographic content

74 Section 4(2)(b)(ii) provides that a user-to-user service or a search service is not a regulated user-to-user service or a regulated search service if it is a service of a kind described in Schedule 2. The effect of Schedule 2 is that certain user-to-user and search services which publish or display regulated provider pornographic content and which would otherwise be exempt under Schedule 1, are instead exempt from only the user-to-user and search services duties. Under section 4(4)(c), services which fall within Schedule 2 will still be regulated services subject to the duties imposed by Part 5 of the Act.

Section 5: Disapplication of Act to certain parts of services

75 This section sets out the circumstances in which this Act does not apply to certain parts of regulated services because of the low risk of harm associated with them.

Part 3: Providers of regulated user-to-user services and regulated search services: Duties of care

Chapter 1: Introduction

Section 6: Overview of Part 3

76 This section provides an outline of each of the Chapters contained within Part 3 of the Act.

Chapter 2: Providers of user-to-user services: duties of care

User-to-user services: which duties apply, and scope of duties

Section 7: Providers of user-to-user services: duties of care

77 This section determines which of the duties set out in Part 3 apply to which regulated user-to-user services. The duties on search services are set out in the following Chapter.

78 Subsection (2) lists the duties that all regulated user-to-user service providers must comply with.

79 Subsection (3) provides that providers of particular kinds of regulated user-to-user services are required to comply with additional duties, as detailed in subsections (4) to (6).

80 Subsection (4) lists the additional duties that providers of regulated user-to-user services that are likely to be accessed by children must comply with. Whether or not a service is likely to be accessed by children is determined in accordance with section 37.

81 Subsection (5) lists the additional duties that providers of Category 1 services must comply with. Designation as a Category 1 service is determined by OFCOM's assessment under the provisions in section 95.

82 Subsection (6) lists the additional duties that providers of combined services must comply with in relation to the search engine component of their service.

Section 8: Scope of duties of care

83 Subsection (1) provides that the duties in this Chapter only apply to regulated user-generated content on user-to-user services that also include regulated provider pornographic content. Subsection (2) provides that for combined services (as defined in section 4(7)) the duties in this Chapter do not apply to search content, any other content that may be encountered following a search request, or anything related to the design, operation or use of the search engine.

84 Subsection (3) provides that the duties in this Chapter only relate to the design, operation and use of a user-to-user service in the United Kingdom and, in the case of duties expressed to apply in relation to users of such a service, how its design, operation and use affects users in the United Kingdom.

Illegal content duties for all user-to-user services

Section 9: Illegal content risk assessment duties

85 This section sets out the risk assessment duties on all providers of regulated user-to-user services in relation to illegal content. Providers must carry out a suitable and sufficient risk assessment by the relevant deadline specified in Schedule 3.

86 Subsection (3) requires the service provider to keep the risk assessment up to date, including when OFCOM significantly changes a risk profile which applies to it.

87 Subsection (4) requires the service provider to carry out a further risk assessment before significantly changing the design or operation of the service.

88 Subsection (5) lists the factors that the service provider must assess, including several factors relating to the likelihood of users encountering illegal content or the service being used for the commission or facilitation of a priority offence, and the severity of the impact this would have on users. It requires the provider to take into account OFCOM's risk profiles (published under section 98) relating to the kind of service it provides.

89 The findings of the provider's risk assessment, including its conclusions about the levels of risk, inform the steps it must take to comply with its safety duties to protect individuals from illegal content under section 10.

90 OFCOM have a duty under section 99 to issue guidance to assist service providers to carry out their risk assessments.

Schedule 3: Timing of providers' assessments

91 Part 1 of Schedule 3 specifies the deadlines by which service providers must complete their illegal content risk assessments and children's access assessments.

92 The general approach is that service providers will have three months from the publication of the guidance relating to a particular assessment (or, once guidance has been published, from the date on which they become a service that needs to complete a particular assessment) to complete the relevant assessment. Part 2 of the Schedule specifies deadlines for children's risk assessments. Under Part 3 OFCOM may extend these deadlines for individual service providers or groups of service providers.

93 Part 3 of Schedule 3 sets out the deadlines by which risk assessments and child access assessments must be carried out by providers of video-sharing platform (VSP) services currently regulated by Part 4B of the Communications Act 2003. These services are subject to transitional arrangements pursuant to which they are obliged to undertake their risk and child access assessments before transitioning from the VSP regime to the Online Safety regime. The requirement to do the assessments is triggered by the assessment start date as set out in Schedule 3, paragraph 8. The general approach is that these services will have three months from the date that the requirement to conduct the assessments is imposed upon them or the date on which the guidance relating to a particular assessment is published, whichever is later.

Section 10: Safety duties about illegal content

94 This section sets out the duties on all providers of user-to-user services with regard to illegal content on their service.

95 Subsection (2) imposes a duty on providers to take proportionate measures relating to the design or operation of the service:

a. To prevent individuals from encountering priority illegal content by means of the service.

b. To mitigate and manage the risk (as identified in the most recent illegal content risk assessment carried out under section 9) of the service being used for the commission or facilitation of a priority offence.

c. To mitigate and manage the risks of harm to individuals identified in the most recent illegal content risk assessment.

96 Subsection (3) requires service providers to use proportionate systems and processes designed to minimise the length of time for which any priority illegal content is present on their services and ensure that any illegal content is swiftly taken down once they become aware of its presence.

97 Subsection (4) provides that the duties in subsections (2) and (3) apply to the way the service is designed, operated and used, as well as to the content present on it. This subsection also lists areas within which the service provider may be required to take or use measures, if proportionate, to comply with their illegal content safety duties. These areas include arrangements for compliance and risk management, service design including design of algorithms (e.g. changing the design of algorithms to prevent users from being directed to illegal content), policies on access and use (e.g. preventing repeat offenders using their services), content moderation (e.g. content removal), user empowerment and support measures and staff policies.

98 Subsections (5) and (6) impose obligations on providers to state in their terms of service how individuals are to be protected from illegal content and to apply these provisions of their terms of service consistently.

99 Subsection (7) specifies that the service provider must include information in its terms of service about any proactive technology that it uses to comply with its duties in respect of illegal content.

100 Subsection (8) sets out that the terms of service provisions required by subsections (5) and (7) must be clear and accessible.

101 Subsection (9) specifies that Category 1 providers must summarise the findings of their most recent illegal content risk assessments in their terms of service. The summary must include the risk assessment findings about levels of risk, and nature and severity of potential harm to individuals.

102 Subsection (12) signposts the fact that the duties about users' rights to freedom of expression and privacy in section 22 are relevant to the illegal content safety duty in this section.

User-to-user services likely to be accessed by children

Section 11: Children's risk assessment duties

103 This section sets out the children's risk assessment duties for user-to-user services that are likely to be accessed by children.

104 Subsection (5) requires service providers to notify OFCOM about content they identify that is harmful to children but does not fall under any categories of content specified as primary priority or priority content that is harmful to children under sections 61 and 62, as well as the incidence of such content on the service.

105 Subsection (6) lists the factors that the service provider must consider as part of their children's risk assessment. This requires services to specifically consider how the design of the service, such as its functionalities and algorithms, affects the level of risk of harm to children. This includes, for example, how easily and quickly content can be shared and the use of features and functionalities which affect how much children use the service. This subsection requires the provider to take into account the risk profile (which would be published by OFCOM under section 98) that relates to the kind of service it provides.

106 This section is not intended to capture risks of harm arising from breaches of existing data protection law.

107 OFCOM have a duty under section 99 to issue guidance to assist service providers to carry out their children's risk assessments.

Section 12: Safety duties protecting children

108 This section sets out the duties on providers of user-to-user services with regard to content that is harmful to children but is not illegal. User-to-user services that are likely to be accessed by children (see section 37) must comply with these duties.

109 Subsection (2) imposes a duty on service providers to take proportionate steps relating to the design and operation of the service:

a. To mitigate and manage the risk of harm to children in different age groups from risks identified in the most recent children's risk assessment carried out under section 11.

b. To mitigate the impact of harm to children in different age groups from content that is harmful to children. This could include user support measures, such as signposting child users to sources of support if they have experienced harm on the service.

110 Subsection (3) requires service providers to use proportionate systems and processes designed to prevent children of any age from accessing primary priority content (as set out in section 61) on their service. It also requires service providers to protect children in age groups which are judged to be at risk from other content that is harmful to children (either priority content as set out in section 62 or other content that satisfies the definition of content that is harmful to children in section 60(2)(c)) on their service.

111 Subsection (4) requires user-to-user service providers to use age verification or age estimation (or both) to prevent children from encountering identified primary priority content that is harmful to children on their service. This duty applies unless the conditions under subsection (5) are met, which includes where the terms of service indicate that that kind of content is prohibited for all users. Where the requirement does apply, under subsection (6) the age verification or age estimation used must be highly effective at correctly determining whether or not a particular user is a child.

112 The duties described in subsections (2) and (3) apply to all areas of the service, including the way the service is designed, operated and used, as well as to the content present on it. Subsection (7) clarifies that age verification or age estimation may be used to comply with duties under subsections (2) or (3), in circumstances where no duty to use age verification or age estimation applies.

113 Subsection (8) lists areas within which the service provider may be required to use measures, if proportionate, to comply with the safety duties for protecting children. These areas include arrangements for compliance and risk management, service design, policies on access and use (e.g. preventing children from accessing specific content on the service), content moderation (e.g. content removal), user empowerment and support measures and staff policies.

114 Subsection (9) requires providers to state in their terms of service how children are being prevented from encountering primary priority content and protected from encountering priority content on their service. It also requires providers to set out how children are protected from encountering other content that would satisfy the definition of content that is harmful to children in section 60. These terms must be applied consistently and must be clear and accessible (subsections (10) and (13)).

115 Subsection (11) specifies that where a provider prevents access to part of, or the whole of the service for users under a particular age, it is required to set out in its terms of service the measures it uses to do so. It is also required to apply those provisions consistently.

116 Subsection (12) specifies that information about any proactive technology the service provider will use to comply with its duties under subsections (2) and (3) must be included in the terms of service.

117 Subsection (14) requires Category 1 services to summarise the findings from its most recent children's risk assessment in its terms of service.

Section 13: Safety duties protecting children: interpretation

118 This section sets out how the child safety duties in section 12 are to be interpreted.

119 Subsection (1) specifies factors which are particularly relevant in determining whether steps, systems and processes are proportionate. Subsection (2) makes clear that services are only required to fulfil the duty in section 12 in relation to the kinds of non-designated content (i.e. content that is neither primary priority content nor priority content but which would satisfy the test of being harmful to children in section 60(2)(c)) if risks from such content have been identified in the most recent children's risk assessment.

120 Subsection (3) explains that references in section 12 to children judged to be in age groups at risk of harm from content that is harmful to children, are to be read as being those who have been assessed as such by the provider in its most recent children's risk assessment.

121 Subsection (4) provides that the duties in section 12(3) and 12(9) (which require service providers to take steps to prevent or protect children from encountering harmful content and to specify those steps in their terms of service) apply only in relation to content which gives rise to a risk of harm due to its nature. It would not be feasible for providers to fulfil these duties for content that is only harmful by the fact of its dissemination. An example would be doxxing, where the content is not inherently harmful to children encountering it but its dissemination may be harmful to a particular targeted child. However, under section 12(2) companies have a duty to mitigate and manage the risks of harm to children on their service, including harm caused through the dissemination of content.

122 Subsection (5) clarifies that the duties which are set out in section 12 extend only to those parts of the service which it is possible for children to access. Under subsection (6), a provider can only conclude that children cannot access a service, or part of a service, if age verification or age estimation is used on the service with the result that children are not normally able to access it.

123 Subsection (8) signposts the fact that the duties about users' rights to freedom of expression and privacy in section 22 are relevant to the safety duties for services likely to be accessed by children in this section.

Section 14: Assessment duties: User empowerment

124 This section requires providers of Category 1 services to carry out (in subsection (2)) and keep up to date (in subsection (3)) assessments in relation to content covered by their user empowerment duties under section 15(2).

125 Subsection (4) requires providers of Category 1 services to carry out an additional assessment of the impacts of any proposed significant change to the service's design or operation, before making the change.

126 Subsection (5) lists the matters which must be covered by these assessments. This includes an assessment of the incidence of relevant content on the services, the likelihood of adult users encountering it, and various factors which may influence that incidence or likelihood.

127 Sections 15(8) and 16(1) make further provision about assessments under this section.

Section 15: User empowerment duties

128 This section sets out the duties on providers of Category 1 services to provide adult users with "control features" to increase their control over certain categories of content, and features to limit their interaction with non-verified users.

129 Under subsection (2) and (3), providers of Category 1 services must, to the extent it is proportionate, have features (defined by subsection (4) as "control features") in place to allow adult users control over certain kinds of content specified in section 16. Section 16 also makes further provision about what is proportionate for this purpose. If a user decides to apply these control features, the service must use systems and processes which either reduce the likelihood of that user seeing the specified kinds of content, or alert that user to the nature of the content.

130 Subsection (5) imposes a duty on providers of Category 1 services to ask all registered adult users to confirm, at the earliest possible opportunity, whether they wish to opt in or out of the use of each control feature the service offers. Subsection (6) sets out that providers must continue to seek this confirmation until the user has made a choice for every control feature.

131 Subsection (8) requires Category 1 services to publish a summary of the findings of their most recent section 14 assessment in their terms of service.

132 Under subsection (9) and (10) providers of Category 1 services must provide users with features to filter out content from non-verified users. If a user applies these features, the service must use systems or processes designed to effectively prevent non-verified users from interacting with that user's content, and reduce the likelihood of that user encountering content from non-verified users.

Section 16: User empowerment duties: interpretation

133 This section aids in the interpretation of section 15 and sets out the kinds of content to which the duty in section 15(2) applies.

134 The duty in section 15(2) requires providers of Category 1 services to offer adult users control features to the extent that it is proportionate to do so. Subsection (1) specifies factors which are particularly relevant to determining what is proportionate for that purpose. These factors are the findings of the most recent assessment under section 14, as well as the size and capacity of the service provider.

135 Subsection (2) sets out the requirements for content to be in scope of subsection (2) of section 15. It must be regulated user-generated content on the service in question and content in subsections (3), (4) and (5).

136 Subsections (2), (3), (4) and (5) specify the content that section 15(2) applies to. This is content which is regulated user-generated content in relation to the service in question, and which: encourages, promotes or provides instructions for suicide, acts of deliberate self-injury or eating disorders; or is abusive or incites hate on the basis of race, religion, sex, sexual orientation, disability, or gender reassignment. These definitions do not capture mere discussion of these topics.

137 Subsections (7), (8) and (9) clarify the meanings of certain terms used in this section and section 15. Subsection (7) also sets out the definition of a non-verified user for the purpose of section 15, making it clear that it includes users outside of the United Kingdom. This would ensure that, if a user decided that they no longer wished to interact with users who have not verified their identities, they would be able to filter out non-verified users regardless of whether those users are based in or outside the UK.

138 Subsection (10) makes clear that the duties under section 22 about privacy and freedom of expression are relevant to the user empowerment duties.

Section 17: Duties to protect content of democratic importance

139 This section sets out the duties on providers of Category 1 services to protect content of democratic importance on their services.

140 Subsection (2) places a duty on providers of Category 1 services to take into account the importance of freedom of expression when designing proportionate systems and processes for taking decisions about content of democratic importance or about users who post such content. This includes decisions about whether to take the content down, to restrict access to it or to take action against a user of the service. For example, providers of Category 1 services could adopt processes to identify democratically important content and ensure users have access to this, even where it might otherwise be voluntarily removed (i.e. for non-compliance with the providers own terms of service, rather than as otherwise required by the Act's safety duties).

141 Subsection (3) requires providers to apply these systems and processes in the same way to a wide diversity of political opinion. This is to ensure that providers of Category 1 services do not privilege some political opinions over others when deciding how to protect content of democratic importance.

142 Subsection (4) requires providers to set out in terms of service the policies and processes designed when complying with subsection (2).

143 Subsection (5) requires that these terms of service are clear and consistently applied. The intention is that the terms of service should be easily understandable for users and that similar decisions are taken about the treatment of similar pieces of content.

144 Subsection (7) defines "content of democratic importance" as news publisher content or regulated user-generated content, both defined under section 55, which is, or appears to be, specifically intended to contribute to democratic political debate in the United Kingdom or in any part or area of the United Kingdom. Examples of such content would be content promoting or opposing government policy and content promoting or opposing a political party.

Section 18: Duties to protect news publisher content

145 Subsection (2) places a duty on Category 1 service providers to take certain steps with regard to recognised news publishers, as defined in section 56, before removing or moderating their content or taking action against their account.

146 Subsection (3) sets out the steps the provider must take before removing or moderating content or taking action against a recognised news publishers' account. This includes notifying the news publisher of the intention to take a particular action. This notification must be in writing (as set out in section 236(1)). The notification must also set out reasons for any proposed action by referring to specific, relevant provisions of the service's own terms of service.

147 Subsections (4) and (5) set out certain circumstances where a provider can take action in relation to recognised news publisher content without following the steps at subsection (3). These are if the provider reasonably considers that continuing to host the content in question would give rise to criminal or civil liability for the service or where the content amounts to a relevant offence as defined by the Act. Subsection (10) clarifies that judgements about whether content amounts to a relevant offence must be taken in accordance with the approach set out in section 192. OFCOM's guidance on illegal content judgements under section 193 may also be relevant.

148 Subsection (7) sets out the steps the provider must take if it takes action in relation to recognised news publisher content without taking the steps set out at subsection (3). The notification must be in writing (as set out in section 236(1)).

149 Subsection (8) specifies that if a recognised news publisher has already been banned from using a service either before the regulatory framework came into force, or after the process in (3) has been followed, and the ban is still in force, the provider may take action against its content without following the steps at subsection (3) and (7). This provision does not enable Category 1 service providers to ban a recognised news publisher once the regulatory framework is in force without following the process in subsection (3) in the first instance.

150 Subsection (9) specifies the circumstances where a provider should not be regarded as taking action in relation to recognised news publisher content. This applies where a provider takes action against content that is not recognised news publisher content, but such content is

impacted and it is not feasible for the provider to separate the recognised news publisher content; and where a provider takes action against an account and that action impacts recognised news publisher content that has been uploaded or shared by the relevant user.

151 Subsections (13) to (15) define 'taking action' in relation to content for the purposes of this section. They make clear that the duty to offer the recognised news publisher an appeal arises when a provider wishes to take down news publisher content, add warning labels to it (other than warning labels normally encountered only by child users), or take any other action on the grounds that it is content which the service's terms of service indicate is not tolerated on the service or is tolerated but liable to be treated in a way which makes users less likely to encounter it. The notification duty under subsection (2) does not therefore apply in relation to other activities by providers such as routine content curation.

Section 19: Duties to protect journalistic content

152 This section sets out the duties on providers of Category 1 services with regard to protecting journalistic content on those services.

153 Subsection (2) places a duty on providers of Category 1 services to take into account the importance of free expression when designing proportionate systems and processes for taking decisions about journalistic content, or about users who post such content. This includes decisions about whether to take the content down, to restrict access to the content or to take action against a user of the service. For example, providers of Category 1 services could adopt procedures to identify journalistic content and ensure users have access to this, even where it might otherwise be voluntarily removed (i.e. for non-compliance with the providers own terms of service, rather than as otherwise required by the Act's safety duties).

154 Subsection (3) and (4) require providers of Category 1 services to create a dedicated complaints procedure available to users who generate, upload or share journalistic content on the service and to creators of journalistic content. The procedure must allow users and creators (as defined in subsections (12) and (13)) to challenge decisions to take down or restrict access to journalistic content or to take action against a user because of journalistic content shared, uploaded or generated by the user. The complaints procedure must be expedited. Under subsection (5), if a complaint is upheld, the content must be swiftly reinstated or the action against the user swiftly reversed. These subsections also make clear that providers are not required to make this complaints procedure available to a recognised news publisher in relation to any decision the provider has taken when complying with their duties set out in section 18.

155 Subsection (8) requires that the terms of service about journalistic content are clear and consistently applied. The intention is that the terms of service should be easily understandable for users and that similar decisions are taken about the treatment of similar pieces of content.

156 Subsection (10) defines "journalistic content" for the purposes of Part 3 of the Act as covering both news publisher content and regulated user-generated content, defined in section 55, that is generated for the purposes of journalism, and which is "UK-linked". This includes, but is not limited to, content generated by news publishers, freelance journalists and citizen journalists. Subsection (11) defines the term "UK-linked".

Duties about content reporting and complaints procedure

Section 20: Duty about content reporting

157 Subsection (2) imposes a duty on providers of regulated user-to user services to have content reporting mechanisms in place (Section 31 contains similar provisions relating to search services).

158 All providers of regulated user-to-user services must enable users and other affected persons (as defined in subsection (5)) to report illegal content; and, providers of such services which are likely to be accessed by children must also enable reporting of content that is harmful to children on parts of the service that it is possible for children to access.

159 Subsection (5) sets out a definition of "affected person" which lists the types of people who are not users of a service but who might be affected by content, or who may need to assist others with making a complaint. These people must also be able to use the content reporting mechanisms.

Section 21: Duties about complaints procedures

160 This section sets out the duties regarding complaints mechanisms which apply in relation to providers of regulated user-to-user services (Section 32 contains similar provisions relating to search services).

161 Subsection (2) sets out that services must have a complaints procedure that:

a. allows for complaints to be made relevant to the type of content and the duties on the service.

b. provides for appropriate action to be taken when a complaint is upheld. Examples of appropriate action might include removal of illegal content if flagged, or reinstating content unfairly removed.

c. is easy to access and use, including by children, and that the process is transparent.

162 Subsection (3) sets out that the policies and procedures that govern handling of complaints must be set out in a service provider's terms of service, and these must be easily accessible, including for children. This is to ensure that users and affected persons can easily find and use the complaints policies and procedures.

163 Subsections (4) to (6) set out the types of complaints for which the different categories of service provider must have a complaints procedure. The types of complaint correspond to the types of content that the regulatory framework requires them to address under relevant duties.

Cross-cutting duties

Section 22: Duties about freedom of expression and privacy

164 This section sets out the freedom of expression and privacy duties. This section applies in relation to user-to-user services (Section 33 contains similar provisions relating to search services). The term 'freedom of expression' is defined in section 236 and the definition is, where appropriate, aligned with that in the European Convention on Human Rights.

All services

165 Subsection (2) places a duty on providers of all regulated user-to-user services to have particular regard to the importance of protecting users' legal rights to freedom of expression when deciding on and implementing safety measures to comply with their duties. Examples of measures that services could take to comply with this duty could include ensuring human moderators are adequately trained to assess contextual and linguistic nuance to prevent over-removal of content.

166 Subsection (3) places a duty on providers of all regulated user-to-user services to have particular regard to the importance of protecting users from breaches of law concerning privacy when deciding on and implementing safety measures to comply with their duties. This

encompasses breaches of existing statutory provisions in data protection legislation such as the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, as well as common law rights such as those relating to private and confidential information. The regulator which enforces obligations which arise under data protection law is the Information Commissioner's Office.

167 Service providers can comply with their duties in subsections (2) and (3) by following measures in OFCOM's codes of practice (see section 49(2)). Under paragraph 10 of Schedule 4, OFCOM are required to design recommended measures in light of the importance of protecting users' rights to freedom of expression and protecting users' privacy, and where appropriate, OFCOM should incorporate protections for the same. Where service providers take measures different from those set out in the codes of practice, they are also under an obligation to ensure that they have particular regard to the importance of freedom of expression and user privacy (see section 49(5)). OFCOM are obliged to consult with the Information Commissioner when preparing the codes of practice (see section 41(6)(g)).

Category 1 services

168 Subsection (4) requires providers of Category 1 services to carry out and publish an impact assessment on the impact that any steps which they have taken, or plan to take, to comply with their safety duties have, or will have, on users' rights to freedom of expression and users' privacy. They must also publish a statement specifying any positive steps they have taken to protect users' rights to freedom of expression and privacy in response to this impact assessment (subsection (7)). Subsection (5) requires this impact assessment to consider the effect of their safety measures and policies on the availability and treatment of news publisher content and journalistic content.

169 Subsection (8) clarifies that the use of "safety measures and policies" in this section refers to those designed to secure compliance with (a) section 10 (illegal content), (b) section 12(children's online safety), (c) section 15 (user empowerment), (d) section 20 (content reporting), or (e) section 21 (complaints procedures).

Section 23: Record-keeping and review duties

170 This section sets out the record-keeping and review obligations that apply to providers of regulated user-to-user services.

171 Providers of user-to-user services are obliged to keep a written record of the risk assessments that they carry out. They must also keep written records explaining which of the measures recommended in a code of practice they are taking for the purposes of complying with their duties. Where a provider is taking an alternative approach to that recommended in a code of practice, it must keep a written record explaining what it is doing instead and how that amounts to compliance with the relevant duties.

172 Subsection (6) requires providers to review compliance with the relevant duties regularly and after making any significant change to their service.

173 Subsection (7) provides OFCOM with the ability to exempt categories of providers from the need to keep written records and carry out reviews. It is anticipated that this power could be used for small, low risk services to ensure these service providers do not face an unnecessary regulatory burden. Where OFCOM considers an exemption is no longer appropriate, they may revoke that exemption. Under subsection (8), OFCOM must publish the details of any such exemptions or revocation of exemptions with reasons.

174 Subsections (9) places a duty on Category 1 providers to keep a written record of their assessment required under section 14. Category 1 services' section 14 assessment covers matters such as the incidence of content that falls in scope of their user empowerment duties. Subsection (9) requires that the written record cover all aspects of the assessment, including how it was carried out and the findings.

175 Subsection (10) specifies that Category 1 providers have a duty to, as soon as reasonably practicable after making a record of an assessment as required by subsection (2) or (9), or revising such a record, that they must then supply this in full to OFCOM.

Chapter 3: Providers of search services: duties of care

Search services: which duties apply, and scope of duties

Section 24: Providers of search services: duties of care

176 This section lists (in subsection (2)) the duties which apply to all providers of regulated search services and (in subsection (3)) the additional duties that providers of search services that are likely to be accessed by children must comply with. Whether or not a service is likely to be accessed by children must be determined by the service provider in accordance with section 37.

Section 25: Scope of duties of care

177 Subsection (1) of this section sets out how the duties in Part 3, Chapter 3 apply to providers of a search service. The duties for providers of a search service only extend to the design, operation and use of the search engine in the United Kingdom or, in the case of a duty that is expressed to apply in relation to users of a service, how its design, operation or use affects United Kingdom users of a service.

178 Subsection (2) sets out how the duties in the Chapter apply to the search engine of a combined service. Firstly, where duties in this Chapter require a service to include something in a publicly available statement, the provider of a combined service may set this out in terms of service. Unlike a search service, a combined service has a user-to-user part which will have such terms. Secondly, since the duties in this chapter refer to a "search service" and a "provider of a search service", this provision makes clear that these references are also to the search engine of a combined service (which does not fulfil the definition of a search service). The intention is that duties apply to the search engine of a combined service, and to the provider of that service, in the same way that they apply to a search service and its provider. The references in section 24 are excepted from this provision because the duties on the provider of a combined service in relation to its search engine are set out at section 7(6).

Illegal content duties for all search services

Section 26: Illegal content risk assessment duties

179 This section sets out the risk assessment duties on all providers of regulated search services in relation to illegal content. Providers must carry out a suitable and sufficient risk assessment by the relevant deadline specified in Schedule 3 and keep this up to date.

180 Subsection (4) requires the service provider to carry out a further risk assessment before significantly changing the design or operation of the service such that the impact of the proposed change is assessed.

181 Subsection (5) lists the factors that the service provider must assess, including several factors relating to the likelihood of users encountering illegal content and the severity of the impact this would have on users. It requires the provider to take into account OFCOM's risk profiles (published under section 98) relating to the kind of service it provides when doing so.

182 The findings of the provider's risk assessment, including its conclusions about the levels of risk, inform the steps it must take to comply with its safety duties to protect individuals from illegal content under section 27.

183 OFCOM have a duty under section 99 to issue guidance to assist service providers with carrying out their risk assessments.

Section 27: Safety duties about illegal content

184 This section imposes duties on providers of regulated search services in respect of illegal content. Subsection (2) requires service providers to take proportionate steps relating to the design or operation of the service to mitigate and manage the risks of harm to individuals, as identified in the most recent illegal content risk assessment of the service under section 26.

185 Subsection (3) requires service providers to ensure that they have proportionate systems and processes to minimise the risk of users encountering either priority illegal content or other illegal content that the provider knows about. These systems and processes could include, for example, down-ranking illegal content in search results, ensuring predictive searches do not drive users towards illegal content, and signposting users who search for illegal content towards resources and support.

186 Subsection (4) provides that these duties apply to the way the service is designed, operated and used, as well as to the content present on it. This subsection also lists areas in which the service provider is required to use measures, if it is proportionate to do so, to comply with its illegal safety duties.

187 Subsections (5), (6) and (8) require service providers to set out their policies and procedures for protecting users from illegal content in a clear and accessible publicly available statement and apply them consistently.

188 Subsection (7) specifies that the service provider must include information in a publicly available statement about any proactive technology that it uses to comply with its duties in respect of illegal content.

189 Subsection (9) imposes a duty on providers of Category 2A search services to summarise the findings of their most recent illegal content risk assessments in a publicly available statement. It also specifies a non-exhaustive list of elements that providers of Category 2A services should include in this summary.

Search services likely to be accessed by children

Section 28: Children's risk assessment duties

190 This section sets out the children's risk assessment duties for providers of search services that are likely to be accessed by children. Service providers must carry out a suitable and sufficient children's risk assessment by the relevant deadline specified in Schedule 3 and keep this up to date.

191 Subsection (5) lists the factors that the service provider must assess in the children's risk assessment. Services must consider factors including the extent to which the design of the service, its functionalities and the different ways in which the service is used may impact the level of risk of harm to children on the service. When carrying out its risk assessment, a service must take into account the risk profile that relates to the kind of service it provides.

192 This section is not intended to capture risks of harm arising from breaches of existing data protection law.

193 OFCOM have a duty under section 99 to issue guidance to assist service providers to carry out their children's risk assessments.

Section 29: Safety duties protecting children

194 This section sets out the duties on providers of regulated search services with regard to content that is harmful to children but is not illegal. All providers of regulated search services that are likely to be accessed by children must comply with these duties.

195 Subsection (2) requires service providers to take proportionate steps relating to the design or operation of the service. These service providers must mitigate and manage the risks and impact of harm to children in different age groups, which they have identified in their most recent children's risk assessment of the service under section 28.

196 Subsection (3) requires service providers to ensure they have proportionate systems and processes to minimise the risk of children encountering primary priority content that is harmful to children or other content that is harmful to children in certain age groups. These systems and processes could include, for example: down-ranking content that is harmful to children in search results displayed to child users; ensuring predictive searches do not drive children towards harmful content; and signposting children who search for harmful content towards resources and support.

197 Subsection (4) provides that these duties apply to the way the service is designed, operated and used, as well as to the content that may be accessed via search results. This subsection also lists areas in which the service provider is required to use measures to comply with its child safety duties, if it is proportionate for them to do so.

198 Subsections (5), (6) and (8) require service providers to set out their policies and procedures for protecting children from harmful content in a clear, accessible publicly available statement, and apply them consistently.

199 Subsection (7) specifies that the service provider must include information in a publicly available statement about any proactive technology that it uses to comply with its safety duties for children.

200 Subsection (9) imposes a duty on Category 2A services to summarise the findings of its most recent children's risk assessment in a publicly available statement.

Section 30: Safety duties protecting children: interpretation

201 This section sets out how the child safety duties on search services in section 29 are to be interpreted.

202 Subsection (1) specifies the factors which are particularly relevant in determining whether steps, systems and processes for the purposes of section 29 are proportionate.

203 Subsection (2) specifies that service providers are only required to meet a duty in this section in relation to non-designated content that is harmful to children if risks from such content have been identified in the most recent children's risk assessment. Non-designated content is that which is neither primary priority content nor priority content but which would satisfy the test of being harmful to children in section 60(2)(c).

204 Subsection (3) explains that references in section 29 to children judged to be in age groups at risk of harm from content that is harmful to children, are to be read as being those who have been assessed as such by the provider in its most recent children's risk assessment.

205 Subsection (4) provides that the duties in section 29(3) (which require service providers to take steps to minimise the risk of children encountering search content that is harmful to children) apply only in relation to content which gives rise to a risk of harm due to its nature. It would not be feasible for providers to fulfil these duties for content that is only harmful by the fact of its dissemination. An example would be doxxing, where the content is not inherently harmful to children encountering it but its dissemination may be harmful to a particular targeted child.

206 Subsection (5) clarifies that the duties in section 29 extend only to those parts of the service which it is possible for children to access. Under subsection (6), a provider can only conclude that children cannot access a service, or part of a service, if age verification or age estimation is used on the service, with the result that children are not normally able to access it.

Duties about content reporting and complaints procedures

Section 31: Duty about content reporting

207 This section sets out the duty on regulated search services to operate systems and processes that enable content reporting (see section 20 for the equivalent provisions relating to user-to-user services).

208 Subsection (2) places a duty on providers of services to have systems and processes in place that allow users and affected persons (as defined in subsection (5)) to report content of the kinds listed which are relevant to the service in question.

Section 32: Duties about complaints procedures

209 This section sets out the duties regarding complaint mechanisms which apply in relation to all providers of regulated search services (see section 21 for the equivalent provisions relating to user-to-user services).

210 Subsection (2) sets out the requirements for services' complaints procedures. Subsection (3) provides that the policies and procedures that govern handling of complaints must be set out in a service provider's terms of service, and that these must be accessible for all users, including children. This is to ensure that users and affected persons can easily find and use the complaints policies and procedures.

211 Subsection (4) sets out the types of complaints that must be enabled on all search services.

212 Subsection (5) sets out the types of complaints that must be enabled on search services likely to be accessed by children.

Cross-cutting duties

Section 33: Duties about freedom of expression and privacy

213 This section sets out the freedom of expression and privacy duties that apply in relation to all providers of search services (see section 22 for the equivalent provisions relating to user-to-user services). The term 'freedom of expression' is defined in section 236 and the definition is, where appropriate, aligned with that in the European Convention on Human Rights.

214 Subsection (2) places a duty on all providers of search services to have particular regard to the importance of protecting users' and interested persons' legal rights to freedom of expression when deciding on and implementing steps to comply with their safety duties.

215 Subsection (3) places a duty on providers of all regulated search services subject to the safety duties to have particular regard to the importance of protecting users from breaches of law concerning their privacy when deciding on and implementing safety measures to comply with their duties. This encompasses existing obligations on service providers regarding users' privacy under data protection law, in particular the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, as well as common law rights such as those relating to private and confidential information. The regulator which enforces obligations which arise under data protection law is the Information Commissioner's Office.

216 Service providers can comply with duties in subsections (2) and (3) by following steps in OFCOM's codes of practice. Under paragraph 10 of Schedule 4, OFCOM are required to design recommended steps to be included in codes of practice in light of the importance of protecting users' legal rights to freedom of expression and protecting users' privacy, and, where appropriate, they should incorporate protections for the same. Where service providers take alternative measures to those set out in the codes of practice, they are also under an obligation to ensure that they have particular regard to the importance of freedom of expression and user privacy. OFCOM are obliged to consult with the Information Commissioner when preparing the codes of practice (see section 41(6)(g)).

Section 34: Record-keeping and review duties

217 This section sets out the record-keeping and review obligations that apply to providers of regulated search services.

218 Providers of regulated search services are obliged to keep a written record of the risk assessments that they carry out. They must also keep written records explaining which of the measures recommended in a code of practice they are taking. Where a provider is taking an alternative approach to that recommended in a code of practice, it must keep a written record explaining what it is doing instead and how that amounts to compliance with the relevant duties.

219 Subsection (6) requires providers to review compliance with the relevant duties regularly and after making any significant change to their service.

220 Subsection (7) provides OFCOM with the ability to exempt categories of providers from the need to keep written records and carry out reviews. It is anticipated that this power could be used for small, low risk services to ensure these service providers do not face an unnecessary regulatory burden. Where OFCOM consider an exemption is no longer appropriate, they may revoke that exemption. Under subsection (8), OFCOM must publish the details of any such exemptions or revocation of exemptions with reasons.

221 Subsection (9) specifies the duty Category 2A providers having made a record of a risk assessment, or revising such a record, to supply OFCOM with a copy of the record in full as soon as practicable.

Chapter 4: Children's Access Assessments

Section 35: Children's access assessments

222 This section establishes a requirement for providers of regulated services to assess whether it is possible for children to access the service (or part of it) and, if so, whether a significant number of children use the service (or the relevant part) and/or whether the service (or relevant part) is likely to attract a significant number of users who are children. Where either of the latter two conditions is satisfied, the service provider will be obliged to conduct a children's risk assessment (see sections 11 and 28) and will be subject to the safety duties protecting children (see sections 12 and 29).

223 Subsection (2) specifies that a provider can only conclude that children cannot access a service, or part of a service, if age verification or age estimation is used on the service with the result that children are not normally able to access it.

224 A provider is only required to consider parts of its service that are user-to-user services or search services when assessing the likelihood of children's access.

Section 36: Duties about children's access assessments

225 This section explains when children's access assessments must be carried out. It also specifies that children's access assessments must be suitable and sufficient and that providers must make and keep a written record of each assessment.

226 Providers must also carry out a separate children's access assessment for each of the services they provide, as specified at subsection (5).

Section 37: Meaning of "likely to be accessed by children"

227 This section sets out the three cases in which a regulated Part 3 service is to be considered "likely to be accessed by children" and therefore subject to the children's risk assessment and child safety duties imposed by either sections 11 and 12 (for regulated user-to-user services) or 28 and 29 (for regulated search services).

228 The first case at subsection (2) is when it is both possible for children to access the service and the "child user condition" (referred to in section 35(3)) is met in relation to the service as a whole, or any part of the service which it is possible for children to access.

229 The second case at subsection (4) is when the service provider has failed to complete the first children's access assessment required under section 36(1).

230 The third case at subsection (6) is when, following an investigation into a provider's failure to comply with a duty about children's access assessments, OFCOM concludes that a service should be treated as "likely to be accessed by children". Section 135(4) and (5) empowers OFCOM to give a confirmation decision to a provider if it is satisfied that the provider has failed to comply with such duties.

Chapter 5: Duties about fraudulent advertising

Section 38: Duties about fraudulent advertising: Category 1 services

231 This section sets out duties about fraudulent advertising for providers of Category 1 services. Category 1 service providers must operate their services using proportionate systems and processes designed to prevent individuals from encountering fraudulent advertisements, minimise the amount of time that fraudulent advertising is present, and swiftly remove fraudulent advertising once they are made aware of it through any means. The definition of a fraudulent advertisement to which the duties on providers apply is at subsection (3).

232 Subsection (2) specifies that a Category 1 service provider must include information in its terms of service about any proactive technology that it uses to comply with its duties in respect of fraudulent advertising.

233 Subsection (4) specifies that if a person is the provider of more than one Category 1 service, the duties set out in this section apply in relation to each such service.

234 Subsection (5) sets out factors for determining proportionality regarding service providers' systems and processes to comply with the duty about fraudulent advertising. These are a) the nature and severity of potential harm from fraudulent advertisement and b) the degree of control a provider has over the placement of advertisements on the service. This recognises that a provider of a Category 1 service may rely on third party intermediaries to display paid advertisements on its service, and will therefore have less control over measures to prevent posting of fraudulent adverts.

Section 39: Duties about fraudulent advertising: Category 2A services

235 This section sets out the fraudulent advertising duties for providers of Category 2A[11] services. Category 2A service providers must operate their services using proportionate systems and processes designed to prevent individuals encountering fraudulent advertisements in or via search results of the service, minimise the amount of time that fraudulent advertising is present, and swiftly remove fraudulent advertising once they are made aware of it through any means. A fraudulent advertisement to which the duties on providers apply is defined in subsection (3).

236 Subsection (2) specifies that a Category 2A service provider must include information in a publicly available statement about any proactive technology that it uses to comply with its duties in respect of fraudulent advertising.

237 Subsection (4) defines what is meant by references to encountering fraudulent advertisements "in or via search results" of a search service. This includes interacting with a paid-for advertisement in search results, for example by clicking on the fraudulent advertisement in a search result and then being redirected to a web page which was linked to the original fraudulent advertisement. Encountering does not extend to any subsequent interactions with a website, for example leaving the original fraudulent advertisement web page.

---

[11] Search services which meet the Category 2A threshold conditions and are included in the relevant OFCOM register. The providers of these services are under a duty to produce annual transparency reports.

238 Subsection (5) specifies that if a person is the provider of more than one Category 2A service, the duties set out in this section apply in relation to each such service.

239 Subsection (6) sets out factors for determining proportionality regarding service providers' systems and processes to comply with the duty about fraudulent advertising. These are a) the nature and severity of potential harm from fraudulent advertisement and b) the degree of control a provider has over the placement of advertisements on the service. This recognises that a Category 2A service provider may rely on third party intermediaries to display paid advertisements on its service, and will therefore have less control over measures to prevent the posting of fraudulent adverts.

Section 40: Fraud etc offences

240 This section sets out a list of offences that constitute fraud offences in relation to the duties about fraudulent advertising.

241 Subsection (5) states that the relevant inchoate offences also apply to the definition of fraud offences e.g. attempting or conspiring to commit an offence specified in subsection (2), (3) or (4).

Chapter 6: Codes of practice and guidance

Codes of practice

Section 41: Codes of practice about duties

242 OFCOM are required to produce specific codes of practice in relation to the illegal content duties (set out in sections 10 and 27) covering terrorist content and offences (subsection (1)) and child sexual exploitation and abuse content and offences (subsection (2)).

243 Subsection (3) requires OFCOM to produce one or more codes of practice in relation to the relevant safety duties beyond those set out in subsections (1) and (2). How these codes should be structured and organised will be a matter for OFCOM to decide as appropriate. The codes of practice will set out the recommended steps that service providers can take to comply with the relevant duties. The relevant duties are listed in subsection (10).

244 Subsection (4) sets out that OFCOM must produce a code of practice for providers of Category 1 and Category 2A services in relation to the duties set out in Chapter 5 (duties about fraudulent advertising).

245 Subsection (5) allows OFCOM to produce amendments and replacements to the codes of practice or to withdraw a code of practice.

246 When preparing draft codes of practice or amendments to them, subsection (6) sets out the parties whom OFCOM must consult. In preparing certain codes of practice, OFCOM must also consult those with expertise in national security or the enforcement of criminal law which is relevant to online safety matters (subsection (7)). Subsection (8) sets out the codes of practice to which this consultation requirement applies.

247 Subsection (9) sets out that the consultation requirements in subsections (6) and (7) are subject to exceptions where minor amendments are made to the codes of practice (as set out in section 48).

Section 42: Codes of practice: principles, objectives, content

248 This section introduces Schedule 4 which establishes the principles OFCOM must consider when preparing codes of practice, the online safety objectives and the measures that may be recommended by codes of practice. It also contains other provisions related to codes of practice.

Schedule 4: Codes of practice under section 41: principles, objectives, content

249 Paragraph 1 requires OFCOM to consider how appropriate the provisions of codes of practice are for the different kinds of regulated user-to-user and search services and to the differing sizes and capacities of the providers of those services.

250 Paragraph 2 sets out various principles OFCOM must have regard to when preparing or amending a code of practice.

251 Paragraph 3 requires OFCOM to ensure that the measures set out in its codes of practice are compatible with the online safety objectives, which are set out at paragraph 4 for regulated user-to-user services and paragraph 5 for regulated search services.

252 Paragraph 6 clarifies how the objectives for user-to-user services and search services apply to combined services.

253 Paragraph 7 gives the Secretary of State power to make changes to the online safety objectives by regulations subject to the affirmative resolution procedure. Paragraph 8 obliges OFCOM to consider as soon as is reasonably practicable whether they should review and subsequently amend the codes of practice following changes to the online safety objectives.

254 Paragraph 9 imposes obligations on OFCOM relating to the content of their codes of practice. These are that codes of practice for illegal content and children's online safety must include measures in the areas set out in those duties where this is proportionate to the type and size of service providers and to risk (sub-paragraph (5)). Sub-paragraphs (1) and (2) cover user-to-user services and (3) and (4) cover search services.

255 Paragraph 10 requires OFCOM to design measures in the codes of practice in the light of the principles of the importance of protecting users' rights to freedom of expression and privacy, and to incorporate safeguards for these rights where appropriate.

256 Paragraph 11 provides that measures set out in a code of practice may only apply to services that are in the United Kingdom or affect users in the United Kingdom. This means that OFCOM could not set out measures in codes of practice that apply to services that do not operate in the United Kingdom or have United Kingdom users.

257 Paragraph 12 sets out provisions which relate to OFCOM's recommendation of age assurance in codes of practice for the purposes of Part 3 of the Act. It includes relevant principles that OFCOM must have regard to when recommending the use of age assurance, and makes clear that OFCOM must recommend highly effective age verification or age estimation in connection with the duty in section 12(3)(a) (preventing children from encountering primary priority content that is harmful to children). Amongst other matters, OFCOM must have regard to relevant standards set out in the latest version of the code of practice under section 123 of the Data Protection Act 2018 (Age Appropriate Design Code). The Information Commissioner's Office oversees the enforcement of data protection law in the UK and is responsible for the Age Appropriate Design Code.

258 Paragraph 13 sets constraints on how OFCOM may recommend proactive technologies in the codes of practice relating to illegal content, child online safety and fraudulent advertising. OFCOM may only recommend proactive technologies in relation to the duties to tackle illegal content, content that is harmful to children and fraudulent advertising. Any such recommendation must be a proportionate response to the risk. Age assurance technologies are not covered by the principles which OFCOM must have regard to when recommending a proactive technology under the Act, because age assurance technologies are now covered by the principles introduced by paragraph 12. In relation to the accuracy and effectiveness of tools, OFCOM may refer to industry standards or set principles through the codes. A proactive technology measure may not be recommended to analyse user-generated content, or metadata relating to such content, which has been communicated privately.

259 Paragraph 14 allows codes of practice to make provisions that are different for user-to-user and search services and to make different provisions for different kinds of service. It also allows OFCOM to differentiate between services and service providers as appropriate.

260 Paragraph 15 provides that codes of practice can apply to service providers based outside of the United Kingdom.

261 Paragraph 16 specifies that a code of practice for the purposes of this schedule means a code of practice about duties issued by OFCOM under section 41.

Section 43: Procedure for issuing codes of practice

262 This section sets out the procedural requirements for approval of the draft codes of practice.

263 Subsections (1) and (2) set out that OFCOM must submit a draft code of practice to the Secretary of State and, provided the Secretary of State does not intend to issue a direction to OFCOM (see section 44), the Secretary of State must lay the draft code before Parliament.

264 Subsection (3) provides that, once the draft code of practice has been laid before Parliament, Parliament has 40 days within which it may resolve not to approve it. If either House of Parliament makes such a resolution, OFCOM must not issue the draft code and instead must prepare another version of it under section 41.

265 If neither House of Parliament makes such a resolution, OFCOM must issue the code of practice and it will come into force after 21 days.

266 This section applies in the same way to amendments to a code of practice as it does to a new code of practice, but not to minor amendments made under section 48.

267 Subsections (9) to (11) set out a time period of 18 months from the day the Act is passed, within which Ofcom must submit the first draft codes of practice relating to certain duties. Subsection (9) sets out these duties.

268 Subsection (12) allows OFCOM to extend the 18 month period by up to 12 months in relation to any of the relevant draft codes by making and publishing a statement. Subsection (13) sets out that Ofcom's statement must give their reasons for doing this and the period of the extension.

269 Subsection (14) allows OFCOM to publish this statement at the same time as, or incorporate, a statement under section 194(3), which contains similar provision about extending the time period for issuing certain guidance documents.

270 Subsection (15) sets out that a statement cannot be made in relation to a draft mentioned in a particular paragraph of subsection (9) if a statement has previously been made under subsection (12) or section 194(3). In effect, OFCOM may only extend the 18 month period a single time.

Section 44: Secretary of State's powers of direction

271 Subsection (1) confers a power on the Secretary of State to direct OFCOM to modify a draft of a code of practice submitted to the Secretary of State under section 43(1), if the Secretary of State believes that modifications are required for the purpose of securing compliance with an international obligation of the United Kingdom.

272 Subsection (2) confers a power on the Secretary of State to direct OFCOM to modify a draft code of practice submitted under section 43(1) if the Secretary of State believes that modifications are required for exceptional reasons relating to national security, public safety, public health, or relations with the government of a country outside the United Kingdom. This power can be used for any code other than a code relating to terrorism or CSEA.

273 Subsection (3) confers a power on the Secretary of State to direct OFCOM to modify a draft terrorism or CSEA code of practice submitted under section 43(1) if the Secretary of State believes that modifications are required for reasons of national security or public safety, or for exceptional reasons relating to public health or relations with the government of a country outside the United Kingdom.

274 Subsection (4) qualifies this power by providing that, where the Secretary of State has required OFCOM to review a draft code of practice under section 47(2), a direction may not be made under this section requiring OFCOM to modify a draft code of practice unless the Secretary of State believes modifications are required for reasons of national security or public safety.

275 Subsection (5) allows the Secretary of State to direct OFCOM to modify a code of practice, following a review under section 47(2) where OFCOM have decided no change is required and have submitted a statement to that effect under section 47(3)(b), should the Secretary of State still believe that modifications are required for reasons of national security or public safety.

276 Subsection (6) requires that any direction to OFCOM under subsection (5) must be given within a period of 45 days from the day on which OFCOM's review statement is submitted to the Secretary of State, and must make particular reference to OFCOM's review statement.

277 Under subsection (7), a direction made under this section cannot require OFCOM to include a particular step to be recommended to providers of services regulated by Part 3 of the Act in a code of practice. The direction must set out the Secretary of State's reasons for requiring modifications, except where setting out those reasons would be against the interests of national security, public safety, or the relations with the government of a country outside the United Kingdom. The Secretary of State must also, as soon as reasonably practicable publish the direction and lay it before Parliament — unless subsection (8) applies.

278 Subsection (8) sets out that if the Secretary of State considers that publishing and laying a direction before Parliament would be against the interests of national security, public safety, or relations with the government of another country outside the United Kingdom then the direction does not have to be published and laid before Parliament. Instead, the Secretary of State must as soon as is reasonably practicable lay a statement before Parliament stating that a direction has been given, the kind of code to which it relates, and the reasons for not publishing it.

279 Subsection (9) provides that OFCOM must as soon as reasonably practicable comply with a direction made under this section, and sets out what OFCOM must do when sending the modified draft code back to the Secretary of State. This includes publishing a document containing details of the direction — except if doing so would be against the interests of national security, public safety or relations with the government of a country outside the United Kingdom.

280 Subsections (10) and (11) provide that the Secretary of State may direct OFCOM to make further modifications to the draft code of practice. Subsections (1) to (5) and (7) to (9) of this section apply to any further directions.

281 Under subsection (12), once the Secretary of State is content that no further modifications are necessary, they must as soon as reasonably practicable lay the revised draft code of practice before Parliament, along with any document submitted by OFCOM detailing the direction or details of how the draft code of practice has been revised in response to the direction as mentioned in subsection (8)(c), as well as OFCOM's review statement under subsection (5), if relevant.

282 Subsection (13) allows the Secretary of State, with OFCOM's agreement, to remove or obscure information in OFCOM's statement, prior to laying it before Parliament, where the Secretary of State considers that its disclosure would be against the interests of national security, public safety, or relations with the government of a country outside the United Kingdom.

283 Subsection (14) provides that the process set out in this section also applies to amendments to a code of practice submitted to the Secretary of State under section 43(1).

284 Subsection (15) defines "terrorism or CSEA code of practice" in this section as a code of practice under section 41(1) or (2).

Section 45: Procedure for issuing codes of practice following direction under section 44

285 This section explains the affirmative and negative procedures for parliamentary approval of the draft codes of practice and sets out when each of the procedures will be applied.

286 Subsection (1) sets out that this section applies where a draft of a code of practice is laid before Parliament under section 44(12).

287 Subsection (2) sets out that if the draft contains modifications made following a direction from the Secretary of State for reasons of public policy under section 44(1), (2) or (3)(b) then the affirmative procedure applies.

288 Subsection (3) sets out that if the draft terrorism or CSEA code of practice contains modifications made following a direction from the Secretary of State for reasons of national security or public safety under section 44(3)(a), (4), or (5) then the negative procedure applies.

289 Subsection (4) sets out the affirmative procedure, which stipulates that a draft code of practice laid before Parliament under this procedure must not be issued by OFCOM unless the draft has been approved by each House of Parliament. If the draft is approved, then it comes into force 21 days from the day on which it was issued. If the draft is not approved, OFCOM must prepare another draft under section 41.

290 Subsection (5) sets out the negative procedure, which stipulates that a code of practice laid before Parliament under this procedure will be issued by OFCOM after a 40 day period, unless Parliament resolves not to approve it. If Parliament resolves not to approve the draft codes then OFCOM must prepare another draft under section 41.

291 Subsection (6) defines "40 day period" as having the same meaning as is in section 43.

292 Subsection (7) sets out that this section also applies to drafts of amendments of a code of practice laid before Parliament under section 44(12).

Section 46: Publication of codes of practice

293 This section sets out what OFCOM must do once a code is ready for publication. Subsections (1) and (2) state that OFCOM must publish a code of practice or amendments to a code of practice within three days of the code or amendments being issued under section 43 or 45.

294 Subsection (3) requires OFCOM to publish a notice where a code has been withdrawn.

Section 47: Review of codes of practice

295 This section makes provision for review of codes of practice by OFCOM. Subsection (1) requires OFCOM to keep all published codes of practice under review.

296 Subsection (2) gives the Secretary of State the power to require OFCOM to review a code of practice on terrorism or CSEA if the Secretary of State deems it necessary for reasons of national security or public safety; and requires the Secretary of State to notify OFCOM of which category the reasons fall into. OFCOM must then carry out a review and either prepare a draft of amendments to the code of practice if they consider that changes are required or, if not, submit a statement to the Secretary of State explaining the reasons for that conclusion.

297 OFCOM must publish the statement submitted to the Secretary of State as soon as is reasonably practicable after a period of 45 days has elapsed, if the Secretary of State has not given a direction to make modifications under section 44(5).

298 Subsection (6) allows the Secretary of State to make representations to OFCOM regarding the removal or obscuring of information in the statement in the interests of national security, public safety, or relations with the government of a country outside the United Kingdom

Section 48: Minor amendments of codes of practice

299 This section allows OFCOM to make minor amendments to the codes of practice (for example to reflect the changes of the name of a relevant organisation) without needing to comply with the requirements for consultation and parliamentary scrutiny. This flexibility should allow the codes to remain up-to-date.

Section 49: Relationship between duties and codes of practice

300 This section sets out how providers of Part 3 services can comply with their relevant duties under this Act.

301 Subsection (1) states that providers will be treated as complying with their duties if they follow the recommended measures set out in the relevant codes of practice. Subsections (2) and (3) provide that user-to-user service and search service providers are to be treated as complying with their duties to protect users' rights to freedom of expression and privacy if they follow the measures in the codes incorporating safeguards for the protection of freedom of expression and privacy. Separately, subsection (4) makes this provision for providers of Category 1 or Category 2A services in relation to a fraudulent advertising code.

302 A provider is not obliged to follow a code of practice; they may instead take alternative measures to comply with the relevant duties in the legislation.

303 Where a regulated provider seeks to comply with a relevant duty by taking alternative measures to those set out in the codes, they must have particular regard to protecting users' rights to freedom of expression and privacy (subsection (5)). When OFCOM assess compliance when a regulated provider has taken alternative measures to those set out in the codes of practice, they must also consider the extent to which users' rights have been safeguarded (where relevant) (subsection (6)).

Section 50: Effects of codes of practice

304 Subsection (1) provides that not taking or using a measure in a code of practice does not of itself make the provider liable to legal proceedings.

305 Subsection (2) confirms that codes of practice can be used as evidence in legal proceedings. Subsection (3) requires a court or tribunal, when determining a question in legal proceedings, to take into account a provision of a code of practice that was in force at the time relating to the question and appears to the court to be relevant.

306 Subsection (4) puts an equivalent requirement on OFCOM when they determine a question which arises in connection with their exercise of a relevant function.

Section 51: Duties and the first codes of practice

307 This section establishes that duties in respect of which OFCOM must issue a code of practice (under section 41) will only apply once the first code of practice for that duty has come into force. This could mean that different duties will apply at different times, depending on when the relevant code for a particular duty comes into force. This section specifies the relevant duties and the corresponding codes under section 41.

308 Section 46(9) specifies that this section is subject to Part 2 of Schedule 17. This is intended to clarify that a provider of a service currently regulated by Part 4B of the Communications Act 2003 does not need to comply with the safety duties while subject to the transitional arrangements set out in Part 2 of Schedule 17.

Guidance

Section 52: OFCOM's guidance about certain duties in Part 3

309 Subsections (1) and (2) require OFCOM to produce guidance for providers of relevant services on how to carry out their record-keeping and review duties at sections 23 and 34, the children's access assessment duties at section 36 and (for providers of Category 1 services) the duties to protect news publisher content at section 18.

310 Subsection (3) requires OFCOM to consult the Information Commissioner before preparing, revising or replacing guidance relating to the record-keeping and review duties at sections 23 and 34, and the children's access assessment duties at section 36.

311 OFCOM must publish the guidance produced, including any revised guidance (subsection (4)).

Section 53: OFCOM's guidance: content that is harmful to children and user empowerment

312 This section requires OFCOM to produce guidance for providers of relevant services which contains examples of content that OFCOM considers to be (or not to be):

a. primary priority and priority content that is harmful to children, and

b. content to which the duty in section 15(2) applies (i.e. content which is described in section 16(2), (3), (4) and (5)).

313 Ofcom must consult appropriate persons before producing the guidance, and must publish the guidance.

Section 54: OFCOM's guidance about protecting women and girls

314 Subsections (1) and (4) require OFCOM to produce and publish guidance for Part 3 service providers on content and activity that disproportionately affects women and girls. This guidance covers content and activity relevant to user-to-user and search services' duties under Part 3 and Part 4 of the Act, such as the illegal content duties, child safety duties, the provisions regarding complaints and reporting, user empowerment duties and the duties regarding terms of service.

315 Subsection (2) notes that OFCOM has discretion about what it puts into the guidance, but it is likely it would summarise the relevant measures set out in the various codes of practice in one place, and potentially add in additional illustrations of best practice. This would ensure providers could easily consider the measures to protect women and girls in a holistic way.

316 Subsection (3) specifies that OFCOM has a duty to consult with the Victim's Commissioner and Domestic Abuse Commissioner before producing and whilst amending the guidance, as well any other persons it considers appropriate.

Chapter 7: Interpretation of Part 3

Section 55: "Regulated user-generated content", "user-generated content", "news publisher content"

317 This section defines "regulated user-generated content" and describes the types of user-generated content that are exempt from this definition, including "news publisher content". Part 3 duties on regulated user-to-user services apply to "regulated user-generated content".

318 Subsections (3) and (4) define "user-generated content". This is content that is generated by a user of the service, or uploaded to or shared on the service by a user of the service, and which may be encountered by another user (or users) by means of the service. This means that content shared only between a user and the service provider (such as through a customer service chat function) would not fall under the definition of user-generated content.

319 Subsection (5) defines "one-to-one live aural communications". It states that aural communications between two users which are not accompanied by written messages, videos or other visual images (other than identifying content, such as a user name or profile picture) and which are not recordings of such content, are exempt from the definition of "regulated user-generated content". For example, a one-to-one live voice call over an internet service would not count as "regulated user-generated content", but a one-to-one video call or a recording of a call shared on a regulated service would. This exemption is expressed as applying to "aural" communications, rather than just to "oral" communications, in order to cover all audio communications (i.e. speech and other sounds), rather than simply speech. This ensures that one-to-one calls akin to traditional telephony are not in scope.

320 Subsections (6) and (7) define "comments and reviews on provider content" in respect of user-to-user services. This definition encompasses user comments and reviews in relation to all content that is published on a service by the service provider or someone acting on their behalf. These are excluded from the definition of "regulated user-generated content", meaning that user-to-user services have no duties with regard to them. In practice, this means that comments and reviews on recognised news publishers' sites and on many sites selling goods and services are not in scope of the regulatory framework. This exemption does not exclude comments or reviews on user-generated content, such as content posted by third party sellers offering goods or services on online marketplaces.

321 Subsections (8) to (10) define "news publisher content". This includes any content on a service directly generated by a recognised news publisher (as defined in section 56). In addition, it includes content originally published by a recognised news publisher but uploaded to or shared on a service by a user of that service, either in its entirety or by way of a link to the entirety of the material. For example, if a user shares the text of an article copied from a recognised news publisher's website, with no additions or amendments, that text will not count as user-generated content. If a user amends content generated by a recognised news publisher that content will count as user-generated content, as will any user-generated text or images accompanying the news publisher content.

Section 56: "Recognised news publisher"

322 This section defines the term "recognised news publisher". Subsection (1)(a) to (c) provides that the British Broadcasting Corporation, Sianel Pedwar Cymru, and any entity that holds a licence under the Broadcasting Act 1990 or 1996 and which publishes news-related content under that licence will qualify as a recognised news publisher.

323 Subsection (1)(d) adds that any entity that meets the conditions listed in subsection (2) will also be considered a "recognised news publisher", providing it is not an excluded entity under subsection (3) or a sanctioned entity under subsection (4).

324 Subsections (3) and (4) define the excluded and sanctioned entities which will not be covered by the definition of "recognised news publisher" where they would otherwise meet the criteria set out in subsection (2). These are entities that are proscribed organisations under the Terrorism Act 2000 or which support such an organisation, and entities that are subject to sanctions regulations.

325 Subsection (5) defines the conditions under which news-related material can be said to be "subject to editorial control". This relates to the relevant condition for qualification as a "recognised news publisher" in subsection (2)(a)(ii).

Section 57: "Search content", "search results" etc

326 Subsection (2) defines "search content" and sets out the types of content that are exempt from this definition, including paid-for advertisements and content on the website of a recognised news publisher.

327 "Search content" is defined as content that may be encountered in or via search results of a search service or search engine. Search results are the content which is presented to a user of the service by the search engine when they make a search request. Typical examples would be a link to a website or an image on an image search results page. Search results may also include short pieces of text from a website, media in other forms, links which are icons or anything else provided it is presented by the operation of the search engine when a search request is made. Subsection (5) makes clear that references to encountering content "via search results" are references to the content which is presented to a user when they interact with a search result itself, for example by clicking on it. That expression does not extend to content which a user comes across as a result of any subsequent interaction (that is, interaction with anything other than a search result). This means that search content includes content on a webpage that can be accessed by interacting with search results.

328 Subsection (3) defines "search results". "Search" is widely defined in subsection (4) to capture the variety of different ways in which search engines can be operated, including speech-based virtual assistants.

Section 58: Restricting users' access to content

329 This section clarifies the meaning of the expression "restricting users' access to content" for the purposes of Part 3 of the Act, including in relation to the content of democratic importance, journalistic content and news publisher protections (sections 17 to 19). The expression is also used in Part 4 of the Act, in the transparency, accountability and freedom of expression duties (sections 71 and 72), where it has the same meaning as here (see section 74(4)).

330 Subsection (2) makes clear that the expression covers cases where a provider prevents a user from accessing content without that user taking a prior step (such as clicking past a warning notice), or where content is temporarily hidden from a user.

331 Subsection (3) further clarifies that this expression does not cover any restrictions on a user's access to content resulting from the user voluntarily activating any feature of a service (such as activating user empowerment tools), or cases where access to content is controlled by another user rather than by the provider.

Section 59: "Illegal content" etc

332 This section defines "illegal content" as content which amounts to a relevant offence (subsections (2) and (3)).

333 Subsection (4) defines a "relevant offence" as a priority offence (defined in subsection (7) as an offence specified in Schedule 5, 6 or 7) or an offence within subsection (5).

334 Subsection (5) covers any offence which is not a priority offence, which has an individual victim or intended victim, and which is created by an Act of Parliament or by certain other specified kinds of legislation. Subsection (6) excludes certain types of offences from the definition of "relevant offence".

335 Subsection (10) defines priority illegal content as terrorism content, CSEA content or content that amounts to an offence listed in Schedule 7. "Terrorism content" and "CSEA content" are defined in subsections (8) and (9) respectively.

336 Under subsection (11), content does not need to be generated, uploaded or accessed (or have anything else done in relation to it) in any part of the United Kingdom to amount to an offence under this provision. This is the case regardless of whether the criminal law would require any relevant action to take place in the United Kingdom (or a particular part of it).

337 Subsection (12) ensures that content generated by a bot is capable of being illegal content.

338 Subsections (13) and (14) clarify that for user-to-user services and the user-to-user part only of combined services, illegal content, terrorism content, CSEA content and priority illegal content does not have to be present on a regulated service to meet the relevant definitions for these types of content. This provision is necessary to allow service providers to take steps in relation to content which would not otherwise meet these definitions because it had not yet been uploaded to or shared on a service.

339 Content amounting to any offence under the law of England and Wales, Scotland or Northern Ireland which meets the definition under subsection (4) is illegal content (including, as appropriate, priority illegal content) in all parts of the United Kingdom for the purposes of the Act.

Schedule 5: Terrorism offences

340 Schedule 5 sets out the offences that constitute "terrorism offences". These are offences contained in existing domestic legislation, including from the Terrorism Act 2000 and 2006, and the Anti-terrorism, Crime and Security Act 2001. The Act does not introduce any new terrorism offences.

341 Paragraph 1 lists the relevant provisions that apply from the Terrorism Act 2000.

342 Paragraph 2 sets out the relevant section from the Anti-terrorism, Crime and Security Act 2001.

343 Paragraph 3 lists the relevant provisions that apply from the Terrorism Act 2006.

344 Paragraph 4 sets out the offences that constitute an inchoate offence. These offences include attempting or conspiring to commit an offence in the Schedule, or encouraging or assisting, aiding, abetting, counselling or procuring the commission of one of those offences (or in Scotland being involved in the commission of such an offence).

Schedule 6: Child sexual exploitation and abuse (CSEA) offences

345 Schedule 6 sets out the offences, in the component jurisdictions of the United Kingdom, that constitute "CSEA offences". The Act does not introduce any new CSEA offences.

346 Schedule 6, Part 1 lists the relevant CSEA offences in England, Wales and Northern Ireland.

347 Paragraph 1 sets out the offence under the Obscene Publications Act 1959, relating to an obscene article tending to deprave and corrupt others. The inclusion of this offence is for instances in which the article would encourage an individual to commit a CSEA-related offence listed in paragraphs 2, 4, 5, 7 or 8.

348 Paragraph 2 sets out offences with regard to indecent photographs, and pseudo-photographs of children: taking; permitting to be taken; making, distributing or showing, possessing with a view to their being distributed or shown by himself or others; and publishing, or causing to be published, any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs.

349 Paragraph 3 sets out equivalent offences in Northern Ireland regarding indecent photographs, or pseudo-photographs, of children, as set out in the Protection of Children (Northern Ireland) Order 1978.

350 Paragraph 4 lists the offence of possession of any indecent photograph, or pseudo-photograph of a child, as set out in section 160 of the Criminal Justice Act 1988.

351 Paragraph 5 lists relevant CSEA-related offences from the Sexual Offences Act 2003 which can be committed online.

352 Paragraph 6 lists equivalent relevant CSEA-related offences in Northern Ireland from the Sexual Offences (Northern Ireland) Order 2008.

353 Paragraph 7 lists the offence under section 62 of the Coroners and Justice Act 2009 (possession of a prohibited image of a child).

354 Paragraph 8 lists the offence under section 69 of the Serious Crime Act 2015 (possession of paedophile manual).

355 Paragraph 9 lists CSEA-related inchoate offences: the offence of attempting or conspiring to commit an offence specified in this Part (Schedule 6, Part 1); an offence under Part 2 of the Serious Crime Act 2007 (encouraging or assisting) in relation to an offence specified in this Part; and an offence of aiding, abetting, counselling or procuring the commission of an offence specified in this Part.

356 Schedule 6, Part 2 lists the relevant CSEA offences in Scotland. Paragraph 10 sets out the relevant offences under the Civic Government (Scotland) Act 1982: section 52 (indecent photographs etc of children) and section 52A (possession of indecent photographs of children).

357 Paragraph 11 lists relevant CSEA offences from the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005.

358 Paragraph 12 lists relevant CSEA offences from the Sexual Offences (Scotland) Act 2009.

359 Paragraph 13 lists CSEA-related inchoate offences: attempting or conspiring to commit an offence specified in this Part; inciting a person to commit an offence specified in this Part; and aiding, abetting, counselling or procuring the commission of an offence specified in this Part, or being involved art and part in the commission of such an offence.

Schedule 7: Priority offences

360 Content which amounts to the criminal offences which are listed in Schedules 5, 6 and 7 is priority illegal content (see section 59(10). Terrorism and CSEA offences are set out in Schedules 5 and 6 respectively. Schedule 7 lists the other priority offences. Under the regime established by this Act, regulated services are required to take proactive action to identify and minimise users' exposure to such illegal content and activity.

361 Paragraph 39 of Schedule 7 sets out the inchoate offences that also constitute priority offences. These include attempting or conspiring to commit an offence specified in the Schedule, or encouraging or assisting, aiding, abetting, counselling or procuring the commission of one of those offences (or in Scotland being involved in the commission of such an offence).

Section 60: "Content that is harmful to children" etc

362 This section defines "content that is harmful to children".

363 Subsection (2) defines "content that is harmful to children" as primary priority (see section 61) or priority (see section 62) content that is harmful to children or a third category of "non-designated content that is harmful to children" - another kind of content which presents a material risk of significant harm to an appreciable number of children in the United Kingdom.

364 The references to content that presents "a material risk of significant harm to an appreciable number of children in the United Kingdom" means that content need not adversely affect a very large number of children to be classified as harmful to children, but content which may adversely affect only one child or very few children will not be caught by the definition of "content that is harmful to children". "Harm" is itself defined in section 234.

365 Subsection (3) excludes certain types of content from the definition of "content that is harmful to children". These are content where the risk of harm comes from the content's potential financial impact, the safety or quality of goods featured in the content or a way in which a service featured in the content may be performed.

Section 61: "Primary priority content that is harmful to children"

366 This section describes four categories of content which count as 'primary priority' content that is harmful to children for the purposes of Part 3 of the Act. These are pornographic content and content that encourages, promotes, or provides instructions for self harm, eating disorders, or suicide.

367 Under section 12(3), providers of user-to-user services are required to put in place proportionate systems and processes designed to prevent children of all ages from encountering these categories of content. Providers of search services are required by section 29(3) to put in place proportionate systems and processes designed to minimise the risk of children of all ages encountering these categories of content.

Section 62: "Priority content that is harmful to children"

368 This section describes six categories of content which count as priority content that is harmful to children for the purposes of Part 3 of the Act. These categories are: bullying content; content that is abusive or incites hatred on the basis of race, religion, disability, sex, sexual orientation, or gender reassignment; content which encourages serious violence; content which depicts realistic serious violence or graphic injury against a person or animal; content which encourages dangerous stunts and challenges; and content which encourages the self-administration of harmful substances.

369 Under section 12(3), providers of user-to-user services must use proportionate systems or processes designed to protect children in age groups judged to be at risk of harm from content in these categories from encountering such content. Providers of search services are required by section 29(3) to use proportionate systems or processes designed to minimise the risk of children in age groups judged to be at risk of harm from content in these categories from encountering such content.

370 Subsections (10), (11) and (12) define or clarify the meanings of terms used in the description of priority content that is harmful to children.

Section 63: Content harmful to children: OFCOM's review and report

371 This section imposes a duty on OFCOM to carry out reviews of the incidence of content that is harmful to children on regulated user-to-user services and search services, and the severity of harm that children in the UK may suffer as a result. It requires OFCOM to publish reports on the outcomes of these reviews at least every three years, with the first report being published within three years of the Act being passed.

372 Subsection (3) mandates that OFCOM's reports must include advice as to whether it is appropriate to make changes to sections 61 and 62, which define primary priority and priority content that is harmful to children. OFCOM must specify in its reports what changes it would recommend.

Part 4: Other duties of providers of regulated user-to-user services and regulated search services

Chapter 1: User identity verification

Section 64: User identity verification

373 This section places a duty on all providers of Category 1 services to offer adult users the option to verify their identity. Providers have discretion as to which form of identity verification they offer, and must make it clear in their terms of service what form of identity verification is available and how the verification process works.

Section 65: OFCOM's guidance about user identity verification

374 This section requires OFCOM to produce and publish guidance for providers of Category 1 services to assist them in complying with the user identity verification duty in section 64(1).

375 As part of preparing the guidance, OFCOM must take into account the desirability of ensuring that the recommended identity verification measures are accessible to vulnerable users. When preparing the guidance, OFCOM must consult the Information Commissioner, persons with relevant technical expertise, persons representing the interests of vulnerable adult users and anyone else they consider appropriate.

Chapter 2: Reporting Child Sexual Exploitation and Abuse Content

Section 66: Requirement to report CSEA content to the NCA

376 This section sets out the requirement on relevant services to report CSEA content to the National Crime Agency (NCA). The NCA is the organisation responsible for receiving reports from services via secure transmission, processing reports including triaging and disseminating reports to law enforcement and other appropriate agencies in the United Kingdom and internationally.

377 Subsection (1) states that a UK provider of a regulated user-to-user service must have systems and processes in place which are capable of making all detected and unreported CSEA content into a report and that these reports are submitted to the NCA.

378 Subsection (2) places the same requirement on non-UK providers of regulated user-to-user services. Non-UK services are only required to report CSEA content to the NCA where they can establish a UK link, unless that provider is already reporting all CSEA content, including UK-linked CSEA content to overseas law enforcement or an alternative reporting body outside the UK – whether on a mandatory or voluntary basis.

379 It is a service's responsibility to ensure all relevant UK offences are reported to the NCA or reported to another body under an alternative reporting regime, regardless of whether the content constitutes an offence in the country the service is based. If the service starts to voluntarily report these additional offences to the relevant reporting body in their country they will remain exempt from this requirement.

380 Subsection (3) sets out the reporting requirement for UK providers of regulated search services. Search services are required to report CSEA content which they detect during routine web crawling which those services already carry out for business purposes. This element of the reporting duty is separate from safety duties under the Act.

381 Subsection (4) places the same requirement on non-UK providers of regulated search services where there exists a UK link to the CSEA content.

382 Subsection (7) sets out that reports must meet requirements set out in regulations and must be sent to the NCA in the manner, and within timeframes set out in regulations.

383 Subsection (10) states that the requirement to report CSEA content is based on when it is detected, not when the offence occurred. An offence may have occurred before the commencement of this requirement, but if it is detected on or after commencement, the service will need to report it.

Section 67: Regulations about reports to the NCA

384 This section places a duty on the Secretary of State to produce regulations about the reports being made to the NCA.

385 Subsection (2) lists the provisions which may be covered in regulations but is not exhaustive. The information that can or should be reported varies depending on the nature of the service and the offence that has occurred. Services are required to report all and any available information relating to instances of CSEA, including any that help identify a perpetrator or victim.

386 Services need to include information relating to the identity of any individual who is suspected of committing a CSEA offence; information relating to the geographic location of the involved individual or website, which may include the Internet Protocol address or verified address; evidence of the CSEA offence itself, such as indecent images or sexual communications between an adult and a child; and any information relating to a child.

387 Subsection (3) states that regulations may include a requirement for providers to retain data in relation to reports made to the NCA. Further details about this requirement including the type of data, the retention period and any restrictions or requirements about how this data is retained will be included in the regulations.

388 Subsection (4) sets out that the power to require the retention of data includes a power to retain the content itself or metadata and user data associated with any person in relation to a report made by the provider.

389 Subsection (5) requires that before making (including revising), regulations, the Secretary of State must consult the NCA, OFCOM and any other appropriate persons. This may include the Information Commissioner's Office in line with their existing duties under the UK GDPR. Regulations will be adaptable to allow for ongoing technological and industry developments and can be revised as necessary.

Section 68: NCA: information sharing

390 This section amends the definition of "permitted purpose" in section 16(1) of the Crime and Courts Act 2013 to allow the NCA to disclose information to OFCOM for the purpose of its functions under this legislation.

Section 69: Offence in relation to CSEA reporting

391 This section sets out the offence of providing false information in relation to the reporting requirement.

392 Subsection (1) states that an offence has been committed where a person provides false information either knowingly or without regard to its accuracy.

393 Subsections (2) sets out the sentencing for a person who is convicted of this offence in England and Wales, Scotland and Northern Ireland.

Section 70: Interpretation of this Chapter

394 This section provides clarification of terms used in this chapter.

395 Subsection (4) provides clarification of when content is considered "detected". This content may be detected by the service provider through a number of means, including automated monitoring systems (such as hash matching), human moderators or user reports. The requirement to report CSEA content is based on when content is detected, not when the offence occurred.

396 Subsection (5) sets out that content is considered "'unreported" by the service if that service does not meet exemptions listed at subsection (5)(a) and (5)(b) by reporting on to a foreign agency or to the NCA. The reporting to the foreign agency may be on a mandatory or voluntary basis.

397 Subsection (6) describes the term "UK-linked" for the purpose of the reporting requirement. The content may be UK-linked based on the place where content is published, generated, uploaded or shared in the United Kingdom; the nationality of the person suspected of committing the related offence; or where the person suspected of committing the related offence is located in the United Kingdom or where the child who is the suspected victim of the related offence is located in the United Kingdom. Where a non-United Kingdom service is able to establish a United Kingdom link as described in subsection (6), this content must be reported to the NCA if it has not already been reported under alternative voluntary or mandatory reporting regimes. The information that a service provider has available to them to determine whether CSEA content is linked to the United Kingdom will vary depending on the nature of that service and the information they collect on their users. The legislation does not specify how services could determine location, but this can be determined through multiple indicators, which may include IP addresses, Media Access Control (MAC) addresses, information provided by users on their profiles, etc.

398 There will not be a consequence if the provider reports CSEA content to the NCA which the provider thinks might have a link to the United Kingdom, but does not.

399 The term "foreign agency" noted at subsection (7) denotes the exemption for services who report under alternative voluntary or mandatory reporting outside of the United Kingdom.

Chapter 3: Terms of service: Transparency, accountability, and freedom of expression

Section 71: Duty not to act against users except in accordance with terms of service

400 This section provides that Category 1 service providers may only remove or restrict access to content, or ban or suspend users, where doing that is consistent with their terms of service or where they face another legal obligation to do so.

401 Subsection (1) sets out the duty on Category 1 service providers to have systems and processes designed to ensure they only remove or restrict access to content, or ban or suspend users, where this is consistent with their terms of service.

402 Subsection (2) provides that the duty in subsection (1) does not apply to actions taken as a result of providers' compliance with their illegal content duties and child safety duties. Actions taken to avoid criminal or civil liability are also exempt from the duty in subsection (1).

403 Subsection (3) sets out that the duty in subsection (1) also does not apply to the removal or restriction of access to content that constitutes an offence, or against a user who has uploaded, generated or shared content that constitutes an offence. Subsection (1) also does not apply where a service bans or suspends a user responsible for or involved in placing fraudulent advertisements on their service. Subsection (7) defines "offence" and "fraudulent advertisement"' for the purposes of this section. It also defines "criminal or civil liability".

404 Subsection (4) exempts consumer content and terms of service about such content from the duty in subsection (1). Section 74(3) defines consumer content as: (a) all regulated user-generated content that is directly connected with the sale of goods or supply of services by consumers and traders who are users of a service, (b) all regulated user-generated content that amounts to an offence under the Consumer Protection from Unfair Trading Regulations 2008, and (c) any other regulated user-generated content that is covered by those Regulations. Such content is already regulated by the Competition and Markets Authority and other consumer protection bodies. The exclusion avoids regulatory overlap between OFCOM and those bodies, and ensures that the duties in this section do not inadvertently create a barrier for the enforcement of consumer protection legislation.

Section 72: Further duties about terms of service

405 This section imposes further duties about terms of service on regulated user-to-user service providers and Category 1 service providers.

406 Subsection (1) requires all providers of regulated user-to-user services to include a provision in their terms of service informing users about their right to bring a claim in court for breach of contract where their content is taken down or access to it, restricted or they are suspended or banned in breach of the terms of service. This seeks to increase transparency about users' existing legal rights; it does not create a new right of action.

407 Subsection (3) requires Category 1 service providers to put in place systems and processes to enforce any terms of service that they set relating to the prohibition of or restriction of access to legal content, and the banning or suspension of users.

408 Subsection (4) requires that such terms of service are clear and accessible. These terms must be easy for users to understand and be written with sufficient detail so users know what to expect in relation to moderation actions taken by the provider. Providers of Category 1 services must also apply their terms of service consistently so that moderation decisions are made in the same way for similar pieces of content.

409 Subsections (5)-(8) require Category 1 service providers to ensure their users can report any content or accounts that the user deems to violate the service's terms of service, and are able to make complaints about providers' moderation actions and compliance with their duties under this section. Providers are required to take appropriate action in response to complaints. The complaints procedure must be easy to use, easy to access, transparent, and specified in terms of service.

410 Subsection (9) excludes terms of service in relation to the illegal content and child safety duties from the duties in this section, as well as terms of service about consumer content. Consumer content is defined in section 74(3), and related terms of service are exempt from these duties because they are already regulated by the Competition and Markets Authority and other consumer protection bodies.

Section 73: OFCOM's guidance about duties set out in sections 71 and 72

411 This section requires OFCOM to produce and publish guidance for Category 1 service providers to help them comply with their duties in sections 71 and 72(3) to (7).

Section 74: Interpretation of this Chapter

412 This section clarifies terms used in sections 71 and 72.

413 Subsection (2) sets out that 'regulated user-generated content' has the same meaning as in Part 3 of the Act.

414 Subsection (3) defines 'consumer content' for the purposes of sections 71(4) and 72(9).

415 Subsection (4) provides that references to 'restricting users' access to content' in this Chapter are to be understood in accordance with sections 57 and 236(6).

416 Subsection (5) sets out the definition of 'relevant content' for the purposes of section 72(5) and (9). This covers regulated user-generated content that a term of service (other than one relating to the illegal content and child safety duties, or consumer content) states that a provider may or will take down or restrict users' access to.

417 Subsection (6) sets out the meaning of an 'affected person' for the purposes of the user redress provisions in section 72(8).

418 Subsection (7) sets out that the size and capacity of a Category 1 service provider are particularly relevant when deciding what steps are proportionate for a service provider to take to comply with its duties under sections 71 and 72.

Chapter 4: Deceased Child Users

Section 75: Disclosure of information about use of service by deceased child users

419 This section imposes duties on providers of Category 1, 2A, and 2B services to set out their policies on disclosing information to the parents of deceased child users, have a dedicated helpline or section of the service (or similar means) for such parents, provide details about the relevant policies and procedures in their terms of service or a publicly available statement, and respond in a timely manner to requests for information. It also requires the providers to operate a complaints procedure in relation to these duties.

Section 76: OFCOM's guidance about duties set out in section 76

420 This section requires OFCOM to produce and publish guidance to assist providers of Category 1, 2A and 2B services in complying with their duties under section 75.

Chapter 5: Transparency Reporting

Section 77: Transparency reports about certain Part 3 Services

421 This section requires providers of relevant services to publish annual transparency reports and sets out OFCOM's powers in relation to these reports. The information set out in transparency reports is intended to help users understand the steps providers are taking to keep them safe, and to provide OFCOM with the information required to hold them to account.

422 Transparency reports are required from Category 1, Category 2A and Category 2B services, as included in the register of categories of certain Part 3 Services (established under section 95). OFCOM may request different types of information depending on which category a particular service meets the conditions for. The Secretary of State may change by regulations the frequency of production of transparency reports, and must consult OFCOM before doing so.

Schedule 8: Transparency reports by providers of Category 1 services, Category 2A services and Category 2B services

423 Schedule 8 lists matters about which information may be required from Category 1 and Category 2B services (Part 1) and Category 2A services (Part 2) in their transparency reports under section 77. It describes high-level types of information that OFCOM are e able to require a service provider to report on. OFCOM will set out the specific information within these categories that service providers need to report on in a notice. This gives OFCOM the flexibility to tailor the reporting requirements so the information sought is as useful as possible. It also allows OFCOM to account for differences between services in setting the transparency requirements and will allow the requirements to evolve over time.

424 This schedule also sets out various factors that OFCOM must take into account when deciding which types of information to require under section 77. These include the service provider's capacity, the type of service and the functionalities the service offers, the number of users of the service and the proportion of users who are children. This helps ensure that the reporting requirements account for the differences between services and are proportionate. These factors are designed to help ensure the information that OFCOM selects is the most appropriate and proportionate type of information to require from the service provider in question.

Section 78: OFCOM's guidance about transparency reports

425 This section places a requirement on OFCOM to prepare and publish guidance on how they will exercise their power relating to transparency reports. Subsection (1) sets out the matters which must be included in guidance and subsection (2) lists expert bodies and interested parties which must be consulted before preparing this guidance, if OFCOM consider them appropriate consultees. OFCOM must have regard to this guidance when preparing or giving a notice to a provider to produce a transparency report (under section 77) or producing their own transparency reports (under section 159).

Part 5: Duties of providers of regulated services: Certain pornographic content

Section 79: "Pornographic content", "provider pornographic content" "regulated provider pornographic content"

426 This section sets out what content the duties in section 80 apply to.

427 Subsection (2) defines what content is provider pornographic content for the purposes of Part 5 (see section 237 for the definition of "content").

428 It does not include user-generated content (as set out in subsection (7)).

429 Subsection 2(a) makes clear that pornographic content published or displayed on a Part 5 service is provider pornographic content either where software, an automated tool or algorithm is applied by the provider or where an automated tool or algorithm, such as a generative artificial intelligence bot, is made available on the service by a provider.

430 Subsection (3) sets out that "regulated provider pornographic content" does not include text-only content, text-only content that is accompanied by a non-pornographic GIF, emoji or symbol, or paid-for advertisements (see section 207 for the definition of paid-for advertisement), as set out in subsections (4) and (5). Such content would not count as regulated provider pornographic content under the Part 5 duties.

431 Subsection (6) sets out is considered pornographic content that is "published or displayed" for the purposes of this Part. Subsection (7) provides that user-generated content, as defined in section 55 is not to be considered provider pornographic content. This subsection keeps the categories of user-generated content and provider pornographic content mutually exclusive.

Section 80: Scope of duties about regulated provider pornographic content

432 Subsections (1) and (2) set out the providers of internet services which are required to comply with the duties under section 81.

433 Subsection (3) sets out that a service is exempt if it is a user-to-user or search service that is exempt as provided for by Schedule 1 or any internet service described in Schedule 9. A service which is exempt from the Part 3 duties by virtue of Schedule 2 is not exempt from the duties in section 81 unless the service is also a service described in Schedule 9. An example of a type of service which is exempt from Part 3 but in scope of Part 5 is a limited functionality service (for example a service whose only user-to-user functionality is users posting comments about provider content) which publishes regulated provider pornographic content.

434 Subsection (4) sets out when a service "has links to the United Kingdom" for the purposes of this Part.

435 Subsection (5) states that Part 5 does not apply to a part of a regulated service if that part meets the definition of an internal business service in either: (a) paragraph 7(2) of Schedule 1 if it is a Part 3 service, or (b) in paragraph 1(2) of Schedule 9 if it is an internet service which is not a Part 3 service. Part 5 may still apply to the non-internal business service part of the service if that part has regulated provider pornographic content. Further exemptions for internal business services are contained in Schedule 9.

436 The effect of subsection (6) is that the duties of Part 5 do not apply to the part of a regulated service which is an on-demand programme service (ODPS) as defined by section 368A of the Communications Act 2003. Part 5 may still apply to the non-ODPS part of the service if that part has regulated provider pornographic content. Further exemptions for ODPS are contained in Schedule 9.

437 The purpose of the combination of exemptions contained in subsections (5), (6), and paragraphs 2 and 6 of Schedule 9 is to provide for where only part of a service is exempt and the remainder of the service remains in scope of Part 5.

438 Subsection (8) clarifies that a service provider's compliance with the duties in section 81 only applies to the design, operation and use of the service in the United Kingdom.

Schedule 9: Certain internet services not subject to duties relating to regulated provider pornographic content

439 Schedule 9 sets out the providers of internet services which are not subject to the duties on regulated provider pornographic content.

440 This includes services which meet the definition of internal business services (either as a whole or for part of the service) and which are not user-to-user or search services. It also includes services provided by public bodies or services provided for by persons providing education or childcare and internet services which are an on-demand programme service as defined by section 368A of the Communications Act 2003 (either as a whole or for part of the service). Section 80(6) also makes provision for when on-demand programme services are not subject to the duties in section 81.

Section 81: Duties about regulated provider pornographic content

441 Section 72 establishes the duties which apply to providers of services with regulated provider pornographic content as set out in section 80(2).

442 Subsection (2) requires providers of services to use age verification or age estimation (or both) to prevent children from encountering regulated provider pornographic content. Subsection (3) requires the age verification or age estimation used to be highly effective at correctly determining whether or not a particular user is a child. Age verification and age estimation are defined in section 230.

443 Subsection (4)(a) requires service providers to keep an easily understood, written record of the age verification or age estimation measures they have used to comply with the duty in subsection (2). Subsection (4)(b) requires service providers to keep such a record of the ways they have protected users from a breach of any statutory provision or rule of law concerning privacy (including, but not limited to, any such provision or rule concerning the processing of personal data) when deciding on the kinds of age verification or age estimation to be used and how they should be used.

444 Subsection (5) requires providers to make publicly available a summary of the age verification or age estimation measures they are using, and how they are using these measures, to meet the duty in subsection (2).

Section 82: OFCOM's guidance about duties set out in section 81

445 This section requires OFCOM to produce guidance for providers of services within section 80(2) to assist them in complying with the duties under section 81.

446 Subsection (2) sets out what OFCOM must include within guidance under this section. The intention is that the guidance will provide services with practical examples to assist them with complying with their obligations which are set in primary legislation. For example, this subsection requires OFCOM to give examples of the kinds and uses of age verification and age estimation that are, or are not, highly effective in correctly determining whether or not a user is a child. It also ensures that the guidance will provide additional transparency on how OFCOM will determine if a service has complied with its duties under section 82.

447 Subsection (3) sets out principles governing the use of age verification or age estimation with regards to their duty in section 81(2) that OFCOM may elaborate on in guidance for providers.

448 Subsections (4) sets out that guidance for providers regarding their duty in section 81(2) may refer to technical standards for age verification or age estimation where they exist.

449 Subsections (5) to (8) set out requirements for OFCOM relating to consultation, and the review and publication of the guidance.

Part 6: Duties of providers of regulated services: fees

Section 83: Duty to notify OFCOM

450 The cost to OFCOM of exercising their online safety functions will be met by fees charged to providers of regulated services. Regulated providers whose qualifying worldwide revenue is equal to or above the specified threshold figure must notify OFCOM for the relevant charging year as per the requirements set out in section 83(1)(a) and (1)(b). A provider is not required to notify OFCOM if they fall within an exemption. Under section 83(6) OFCOM may provide for exemptions where they consider it appropriate and the exemption is approved by the Secretary of State.

451 Regulated service providers must notify OFCOM and provide supporting evidence within the timeframes stipulated in subsection (5).

452 The evidence which services must provide at the point of notification will be set out in regulations to be made by Ofcom under section 85(2). OFCOM will also define the terms "qualifying worldwide revenue" and "qualifying period" in regulations made under section 85.

Section 84: Duty to pay fees

453 The cost to OFCOM of exercising their online safety functions will be met by fees charged to providers of regulated services. This section empowers OFCOM to require a provider of a regulated service to pay such fees.

454 The fee payable to OFCOM will be determined by reference to the provider's qualifying worldwide revenue for the qualifying period and any other factors that OFCOM consider appropriate.

Section 85: Regulations by OFCOM about qualifying worldwide revenue etc

455 This section sets out details of what OFCOM may make provision for in the regulations about "qualifying worldwide revenue" and "qualifying period" and regulations about information that must be supplied for the purposes of section 84. It also sets out procedural requirements relating to the regulations.

Section 86: Threshold figure

456 OFCOM will be funded via fees from providers of regulated services whose qualifying worldwide revenue is equal to or greater than a specified threshold figure.

457 This section sets out that OFCOM must carry out a consultation to inform the setting of the threshold figure for the purposes of sections 83 and 84. After the completion of the consultation, and having taken advice from OFCOM, the Secretary of State must make regulations specifying the threshold figure for those purposes. Subsections (3)-(7) set out the process to be followed when the threshold is first set and each time it is revised.

Section 87: Secretary of State's guidance about fees

458 This section sets out the requirement for the Secretary of State to issue guidance to OFCOM regarding the principles to be included in their Statement of Principles (see section 88).

459 This section also sets out procedural requirements in respect of the guidance and OFCOM's duties in respect of the guidance when exercising their functions under this Part of the Act.

Section 88: OFCOM's fees statements

460 OFCOM are required to produce a Statement of Principles that it will apply when determining the fees payable by providers of regulated services. OFCOM is not permitted to require providers to pay a fee unless a statement of principles is in force.

461 This section sets out requirements about the principles and what the Statement must include, as well as procedural requirements relating to the Statement.

462 Subsection (9) also makes clear that OFCOM's costs include costs incurred by OFCOM in preparation for the exercise of their online safety functions during a charging year.

Section 89: Recovery of OFCOM's initial costs

463 This section introduces Schedule 10.

464 Schedule 10 provides a mechanism whereby the costs incurred by OFCOM in undertaking work which directly or indirectly prepares OFCOM for their future role as the online safety regulator prior to the commencement of section 88 of the Act can be recovered by way of fees charged to providers of regulated services. In accordance with section 401(1) of the Communications Act and OFCOM's statement under that section, OFCOM have retained Wireless Telegraphy Act receipts to meet these costs.

465 Schedule 10 allows OFCOM to recover, from providers of regulated services, an amount equivalent to the amount of Wireless Telegraphy Act receipts OFCOM have retained to meet the costs incurred on preparations for the exercise of their online safety functions before the day on which section 88 comes into force.

Schedule 10: Recovery of OFCOM's initial costs

466 This Schedule requires OFCOM to seek to recover their "initial costs", which are defined at paragraph 1(3)(a).

467 Paragraph 1 makes it clear that the amount to be recovered is the amount of Wireless Telegraphy Act (WTA) receipts retained by OFCOM to meet those costs. The first phase of this process is set out in paragraph 2. OFCOM will charge additional fees over a number of years, beginning after the initial charging year. The aggregate of those fees will equal the total of OFCOM's initial costs. Paragraph 7(5) sets out that that period will be no less than 3 and no more than 5 years.

468 Once that phase has been completed, there will be a second phase, as set out in paragraph 3. In the first year of the second phase OFCOM will charge fees to recover the outstanding amount, which is the amount of the additional fees yet to be recovered, which OFCOM consider are not likely to be paid or recovered, less any amount specified by the Secretary of State under paragraph 3(5). This process is repeated if necessary until all the money is either recovered, or OFCOM consider it is likely to be recovered, or the Secretary of State makes a determination under paragraph 4(2) that it does not need to be recovered. Paragraph 5 enables OFCOM to refund part of a fee where a provider is only a regulated service for part of a year.

469 Under paragraph 7 the Secretary of State must make regulations providing details of the additional fees, including the initial costs, the charging years, and the computation model. Before doing so they must consult OFCOM and regulated service providers.

Section 90: Meaning of "charging year" and "initial charging year"

470 This section sets out the definitions of ''charging year'' and ''initial charging year''.

Part 7: OFCOM's powers and duties in relation to regulated services

Chapter 1: General Duties

Section 91: General duties of OFCOM under section 3 of the Communications Act

471 This section amends OFCOM's existing general duties under section 3 of the Communications Act 2003 (CA 2003), in order to set out duties applicable to OFCOM's new role as the online safety regulator.

472 This section introduces a new general duty on OFCOM to secure, in the carrying out of their functions, the adequate protection of citizens from harm presented by regulated services, through the appropriate use by providers of such services of systems and processes designed to reduce the risk of such harm.

473 The amendments include listing the factors that OFCOM must have regard to in performing the new general duty, and specifying that OFCOM do not need to have regard to the desirability of promoting and facilitating the development of self-regulation in carrying out their functions under the Online Safety Act 2023.

474 This section also provides that the terms 'content', 'harm', 'provider', and 'regulated service' have the same meaning in the CA 2003 as in the Online Safety Act 2023.

Section 92: Duties in relation to strategic priorities

475 This section sets out OFCOM's duties in relation to statements of strategic priorities designated by the Secretary of State under section 153(1).

476 In particular, OFCOM must have regard to any such statement in carrying out their online safety functions.

Section 93: Duty to carry out impact assessments

477 This section extends OFCOM's duty to carry out impact assessments on important proposals under section 7 of the Communications Act 2003 (CA 2003) to their online safety functions.

478 Section 7(2A) of the CA 2003 will provide that all proposals to introduce, replace or amend codes of practice under the Online Safety Act 2023 are "important proposals" for the purposes of OFCOM's duty to carry out impact assessments. This means that OFCOM will either need to undertake and publish an impact assessment on these proposals, or to publish a statement detailing why they consider such an assessment unnecessary.

479 Section 7(4B) of the CA 2003 provides that all assessments of proposals which relate to the carrying out of OFCOM's online safety functions must include an assessment of the likely impact of implementing the proposal on small and micro businesses. If only part of the proposal relates to OFCOM's online safety functions, then only that part must be assessed to determine its likely impact on small and micro businesses.

Chapter 2: Register of categories of regulated user-to-user services and regulated search services

Section 94: Meaning of threshold conditions etc

480 This section sets out how Schedule 11, which provides details about the regulations for establishing threshold conditions, applies in relation to Part 3 Services.

Schedule 11: Categories of regulated user-to-user services and regulated search services: regulations

481 This Schedule sets out the procedure for making and amending the regulations that establish the threshold conditions a relevant service must meet in order to be designated as a Category 1, Category 2A or Category 2B service.

482 Paragraphs 1(1) and (3) state the Secretary of State must make regulations specifying threshold conditions for Category 1 and 2B relating to number of users, functionalities, and any other relevant characteristics and factors. Paragraph 1(2) states the regulations for Category 2A threshold conditions must relate to number of users, and any other relevant characteristics and factors.

483 Paragraph 1(4) provides that these regulations must specify how a service may meet the relevant threshold conditions. It makes clear that, in order to meet the threshold conditions to become a Category 1 or 2B Service, a service must meet as a minimum at least one condition relating to the number of users or at least one condition relating to functionality. The regulations may specify that a service must meet a combination of conditions, for instance conditions relating to both the number of users and the functionalities on offer. For Category 2A Services, a service must meet as a minimum at least one condition relating to the number of users. This ensures that the factors which are set out on the face of the Act as being most important in determining whether it is proportionate to place additional duties on the provider of a user-to-user service or a search service will be reflected in each designation decision.

484 Under sub-paragraphs (6) and (7) of paragraph 1, the Secretary of State, in making regulations under sub-paragraphs (2) and (3), for Categories 2A and 2B, must consider the likely impact the factors set out in the previous sub-paragraphs will have on the level of risk of certain types of harm.

485 Paragraph 2 establishes the procedure for making the first set of regulations under paragraph 1. Sub-paragraphs (2), (3), and (4) of paragraph 2 set out that OFCOM must carry out research to inform the making of these regulations. This research must be carried out within six months of Royal Assent. However, for research in relation to Category 2A and 2B services, paragraph 2(10) allows for the Secretary of State to give OFCOM extra time to carry out the research, up to a limit of 18 months after Royal Assent. Extra time could be required if, for example, the Secretary of State determined that it was necessary to consider the effectiveness of the transparency reporting framework for Category 1 services before extending its scope.

486 OFCOM must then provide advice to the Secretary of State, based on their research, as to what they consider would be the appropriate threshold conditions (paragraph 2(5) of Schedule 11). In respect of Category 1, 2A and 2B threshold conditions, OFCOM may advise that the regulations should include other characteristics or factors in addition to number of users (and, for user-to-user services, functionalities), and what those other characteristics or factors should be.

487 If the regulations include provisions which differ in any material respect from what was advised by OFCOM, the Secretary of State must publish a statement explaining why they have departed from that advice (paragraph 2(8) of Schedule 11).

488 After the regulations are made, OFCOM will be required to assess services which they consider are likely to meet the relevant threshold conditions against the threshold conditions set out in the regulations, and to establish a register of Category 1, Category 2A and Category 2B services (see section 94(1)). Services become subject to Category 1, 2A or 2B duties by virtue of being added to the relevant part of the register.

489 Paragraph 3 establishes the procedure for updating the threshold conditions by amending or replacing regulations made under paragraph 1. Paragraphs 3(1), (2), and (3) state that regulations may only be amended or replaced by further regulations, once OFCOM have carried out further research.

490 Paragraph 3(4) states that either OFCOM or the Secretary of State may initiate the carrying out of this further research and the research should be carried out to the depth that OFCOM consider appropriate.

491 Paragraph 3(6) states that following further research being carried out, OFCOM must advise the Secretary of State whether or not, in OFCOM's opinion, changes to the regulations are appropriate (and, if appropriate, what those changes should be). Paragraph 3(7) notes that OFCOM must publish this advice as soon as reasonably practicable after providing it.

492 To ensure oversight of the process, paragraphs 3(8) and (9) impose duties on the Secretary of State to publish a statement explaining their decision if they take action which departs from OFCOM's advice.

Section 95: Register of categories of certain Part 3 services

493 This section imposes a duty on OFCOM to establish and publish a register of each regulated service that meets the various threshold conditions set out in Schedule 11 and will therefore be designated as a Category 1, 2A or 2B Service.

494 Subsections (5) and (6) set out how services should be treated if they meet the threshold conditions for different categories of service. This can happen either where a user-to-user service (with no search engine) meets both the Category 1 and Category 2B threshold conditions or in the case of a combined service. Where a user-to-user service meets both the Category 1 and Category 2B conditions, it is considered a Category 1 service, and added only to the Category 1 part of the register. As a combined service is a user-to-user service with a search engine part, it is possible that the user-to-user part of the service will meet the threshold conditions for Category 1 or Category 2B and, at the same time, the search engine will meet the threshold conditions for Category 2A. Where this happens, the service is considered both a Category 1 and Category 2A service or both a Category 2B and Category 2A service, and added to both relevant parts of the register. Where a service meets the threshold conditions for all three categories, it is considered both a Category 1 and a Category 2A service and added to these parts of the register.

495 Subsection (9) outlines that OFCOM must take steps to obtain or generate information in order to assess whether Part 3 services meet the threshold conditions.

Section 96: Duty to maintain register

496 This section sets out OFCOM's duties with regard to maintaining the register of regulated services that are designated as either Category 1, Category 2A, or Category 2B. Further detail on the register is set out in section 86.

497 Subsections (1), (2) and (3) state that, for Category 1, Category 2A and Category 2B services respectively, if regulations setting threshold conditions are amended or replaced, OFCOM must conduct a full reassessment of services which they consider are likely to meet the amended thresholds set in the relevant regulations. They must then update the register accordingly. OFCOM must do this as soon as is reasonably practicable after the date on which the amending or replacement regulations are made.

498 Subsection (4) requires OFCOM, at any other time, to assess those services which are not on the register, but which they consider are likely to meet the threshold conditions for designation as a Category 1, Category 2A or Category 2B service, and to add them to the relevant part of the register accordingly if they are assessed to meet the threshold conditions. In practice, this allows OFCOM to respond to changes relating to a regulated service and to ensure that the register remains up-to-date.

499 Subsections (6) to (8) allow providers of a service listed in the register to request the service's removal from the register. If they make such a request, OFCOM must first determine whether they are satisfied, based on the evidence submitted by the provider in question, that there has been a change to the service or to regulations under paragraph 1 of Schedule 10 which appears likely to be relevant. Only if OFCOM are satisfied that this is the case are they obliged to assess the service and notify the provider of their decision. This ensures that OFCOM do not have to

do a full assessment every time a request is made, which could create disproportionate burdens. If OFCOM assess the service and consider that they no longer meet the relevant threshold, OFCOM must remove them from the relevant part of the register.

500 Subsection (9) requires OFCOM to take reasonable steps to obtain or generate information or evidence to inform their assessments of services under this section, in the same way as they are required to do for the original assessments undertaken when the register is first established.

501 Subsection (11) refers to the appeals section of the Act, for provisions about appeals against a decision to either include a service in the register, or a decision not to remove a service from the register.

Section 97: List of emerging Category 1 services

502 This section confers a duty on OFCOM to create and publish a list of companies that are approaching the Category 1 thresholds. This ensures that OFCOM proactively identifies rapidly scaling services and are ready to assess and add these companies to the Category 1 register without delay.

503 Subsection (1) states that OFCOM must comply with this duty as soon as is reasonably practicable after the regulations specifying Category 1 threshold conditions have come into force.

504 Subsection (2) sets out the conditions a service must meet to be added to the list.

505 OFCOM are required to assess services against these conditions and prepare a list of emerging Category 1 services. Subsections (3)–(6) outline how OFCOM must publish and manage this list.

506 Subsection (7) sets out how OFCOM can obtain or generate the necessary information or evidence for the purposes of assessing services for this list.

Chapter 3: Risk assessments of regulated user-to-user services and regulated search services

Section 98: OFCOM's register of risks, and risk profiles, of Part 3 services

507 Subsection (1) of this section places a duty on OFCOM to identify and assess the risks of harm to individuals in the United Kingdom presented by in-scope services. These risk assessments must cover the risks of harm to individuals in the United Kingdom presented by illegal content and content that is harmful to children. Risk assessments for user-to-user services must also cover the risks of harm presented by the use of such services for the commission or facilitation of priority offences. OFCOM must publish a register of risks of Part 3 services which reflects the findings of the risk assessments carried out.

508 Subsection (5) sets out that OFCOM must develop risk profiles for different groupings of regulated services to assist them in complying with their risk assessment and safety duties. OFCOM should categorise these services as they consider appropriate. This must take into account the services' characteristics, which include user base, business model, governance and other systems and processes (see subsection (11)), the risk levels, and any other relevant matters identified in its risk assessment.

Section 99: OFCOM's guidance about risk assessments

509 This section sets out OFCOM's duties to provide guidance for providers of regulated services to assist them with complying with their risk assessment duties.

510 The section sets out the types of guidance that must be prepared, when the guidance must be prepared, and when it must be updated. The section requires OFCOM to consult the Information Commissioner before producing any guidance.

Chapter 4: Information

Information power and information notices

Section 100: Power to require information

511 Subsection (1) gives OFCOM the power to require the provision by a person within the categories listed in subsection (5) of information OFCOM require in order to discharge their online safety functions. For instance, OFCOM could use this power to require a relevant service provider to share a risk assessment in order to understand how that provider was identifying risks. OFCOM must issue an information notice (in accordance with section 102) in order to exercise this power.

512 Subsection (3) makes clear that the power conferred by subsection (1) gives OFCOM the power to require certain providers (those specified in paragraphs (a) to (d) of subsection (5)) to take steps to allow a person authorised by OFCOM to view remotely specific types of information.

513 The power under subsection (3) will allow persons authorised by OFCOM to observe the carrying out of empirical tests, which are a standard method for understanding algorithms and which involve taking a test dataset, running it through an algorithmic system, and observing the output. Under section 102(5) a provider must be given at least seven days to comply with a notice which requires the taking of steps in relation to remote viewing under subsection (3).

514 When exercising the power under subsection (3), Ofcom is only permitted to do so for the purpose of exercising their online safety functions, and is unable to use this power for any purpose other than the viewing of specific types of information. For example, Ofcom may exercise this power for the purposes of assessing compliance with the online safety duties. Given that the power only exists for the purpose of viewing information, OFCOM is unable to directly control the service when exercising this power, nor could they use it to require companies providing infrastructure services to create the means to weaken or circumvent cybersecurity measures.

515 In observing tests under subsection (3), where an appropriate test server is available OFCOM may seek to observe a test using that test server. If a test server is unavailable, OFCOM may request a test using the server that is used to deliver the 'live' service, but they would only be able to view such a test and any data processing would need to comply with data protection law. OFCOM would generally expect to require a service to use a test dataset. OFCOM may request either that the service uses a test dataset provided by OFCOM, or the service uses its own test dataset, when performing a test. Which approach is taken will depend on the circumstances.

516 Subsection (4) places a legal requirement on OFCOM to exercise the subsection (1) power in a way that is proportionate. That means that Ofcom will need to consider how necessary it is for Ofcom to obtain the information before deciding whether to exercise the power. Any technical and operational limitations on viewing information, including the use of cybersecurity measures such as encryption may also be relevant to Ofcom's decision as to whether and when to exercise this power.

Section 101: Information in connection with an investigation into the death of a child

517 This section gives OFCOM the power to require the provision by a person within the categories listed in section 100(5) of information for the purposes of responding to a notice given to OFCOM by a coroner or, in Scotland, a procurator fiscal, in connection with the death of a child, including information about the use of a service by the deceased child.

Section 102: Information notices

518 This section provides further information on OFCOM's information gathering powers. It sets out the details that can, and the details that must, be included in a notice given under section 100(1) or 101(1) requiring the provision of information, and imposes a duty on the recipient of such a notice to comply with it.

519 Among other things, the section clarifies that OFCOM may require the provision of information in any form; that OFCOM may cancel an information notice; and that a person to whom a document is produced, for example an OFCOM employee, can take copies of a document and require an explanation of it. Subsection (5) also makes clear that a provider must be given at least seven days to comply with a notice requiring the taking of steps in relation to remote viewing under section 100(3).

Section 103: Requirement to name a senior manager

520 Criminal proceedings may be pursued against a named senior manager of a regulated service who fails to comply with an information notice (see section 109). This section provides OFCOM with the power to require, in an information notice, that an entity names a relevant senior manager who will then be responsible for ensuring the entity complies with the notice.

521 Subsection (4) defines a "senior manager" as an individual who plays a significant role in making decisions or the managing and organising of the entity's "relevant activities", as defined in subsection (5).

Skilled persons' reports

Section 104: Reports by skilled persons

522 Subsection (1) sets out the circumstances under which OFCOM can require a report from a skilled person. The first scenario (subsection (1)(a)) is for the purpose of identifying and assessing a failure or a possible failure, by a provider of a regulated service to comply with a relevant requirement (as listed in subsection (13)). The second scenario (subsection (1)(b)), which applies only where OFCOM considers that the provider may be at risk of failing to comply with a relevant requirement, is for the purpose of developing OFCOM's understanding of this risk and ways to mitigate it. The third scenario (subsection (3)) is in relation to assisting OFCOM when the regulator is deciding whether to give a notice requiring a provider to use their best endeavours to develop or source technology dealing with CSEA content, or in deciding the requirements to be imposed by such a notice.

523 Subsections (4) and (5) set out that OFCOM may appoint a skilled person (an external third party with relevant expertise) to carry out a report and if they do so must notify the provider, or, alternatively, OFCOM may give a notice to a provider requiring them to appoint a skilled person to produce a report for OFCOM, in the form stipulated by OFCOM, and specifying the relevant matters that must be dealt with in the report.

524 Subsection (7) sets out that the service provider, their employees, their contractors and other providers have a duty to assist the skilled person in any way as the skilled person may reasonably require to prepare the report.

525 Subsection (8) provides that the provider is liable to pay the skilled person directly for the production of the report, which can be recovered through the courts (see subsections (9) to (12)).

Investigations and interviews

Section 105: Investigations

526 This section relates to investigations by OFCOM into whether a provider of a regulated service has failed, or is failing, to comply with a requirement mentioned in subsection (2). Subsection (1) lays down that the provider must cooperate fully with the investigation.

527 Subsection (2) sets out that the requirements cover the list of duties and requirements in section 131 (enforceable requirements) and any requirements imposed by a notice under section 121(1) (notices to deal with terrorism content or CSEA content (or both)).

Section 106: Power to require interviews

528 This section gives OFCOM the power to require certain individuals to attend an interview. Subsection (1) states that this power can be used when OFCOM are carrying out an investigation into the failure, or possible failure, of a provider of a regulated service to comply with a relevant requirement.

529 Subsections (2) and (3) specify what information OFCOM must provide when giving an individual a notice to attend an interview and subsection (4) lists the individuals who can be required to attend an interview.

530 Subsection (5) states that OFCOM must give a copy of the notice to the provider of the service if they give a notice to an officer, a partner or an employee of the provider of the service.

531 Subsection (6) specifies that this section does not require a person to disclose information that would be protected by legal professional privileges (or, in Scotland, to confidentiality of communications) in legal proceedings.

Powers of entry, inspection and audit

Section 107: Powers of entry, inspection and audit

532 This section introduces Schedule 12 to the Act, which makes provision about OFCOM's powers of entry, inspection and audit.

Schedule 12: OFCOM's powers of entry, inspection and audit

Authorised persons

533 Schedule 12 sets out OFCOM's powers of entry, inspection and audit. Paragraph (1) states that OFCOM may authorise persons to exercise their powers of entry and inspection, carry out audits or apply for and execute a warrant.

Power of entry and inspection without a warrant

534 Paragraph 2, sub-paragraphs (1), (2) and (3) set out conditions on OFCOM's powers of entry without a warrant.

535 Sub-paragraphs (4), (5), (6) and (7) list what a person authorised to exercise powers under paragraph 2 may do.

Notice requiring information or documents at inspection

536 Paragraph 3 sets out information about the process associated with an inspection notice.

Audit

537 Paragraph 4 relates to the function of an audit notice. An audit notice may require a regulated provider to take actions mentioned in sub-paragraph (2) to assist OFCOM's audit.

Conditions for issue of a warrant

538 Paragraph 5 deals with the conditions for the issue of a warrant by a justice for the inspection of premises by OFCOM.

Evidence of authority

539 Paragraph 6 states the requirements an authorised person must meet before exercising a power of entry under a warrant.

Powers exercisable by warrant

540 Paragraph 7 lists what a warrant may allow an authorised person to do.

Powers of seizure: supplementary

541 Paragraph 8 deals with powers of seizure (i.e. when a person executing a warrant seizes a document, record or other thing).

Further provision about executing warrants

542 Paragraphs 9 to 15 set out further provisions relating to the execution of a warrant.

Return of warrants

543 Paragraph 16 sets out provisions relating to the return of warrants.

Restrictions on powers

544 Paragraph 17 applies limitations to the powers set out in paragraph (2), relating to entry and inspection of premises without a warrant, and to powers exercisable under a warrant.

Offences

545 Paragraph 18 provides that a person commits an offence if the person intentionally obstructs a person acting under this Schedule or the person fails, without reasonable excuse, to comply with any requirement imposed under this Schedule or knowingly provides false information.

546 Sub-paragraph (2) sets out the penalty of fine and/or maximum sentences that can be imposed by the relevant criminal court on conviction.

Interpretation

547 Paragraphs 19 to 23 define "domestic premises", "premises", person "acting under this Schedule", "enforceable requirement", and "warrant" for the purposes of this Schedule. Paragraphs 23 and 23 provide clarification around interpretation when paragraph (5)(1) is applied in Scotland or Northern Ireland.

Section 108: Amendment of Criminal Justice and Police Act 2001

548 This section confers on OFCOM the additional powers of seizure in section 50 of the Criminal Justice and Police Act 2001, in relation to OFCOM's Schedule 12 powers of seizure under warrant. In certain circumstances, this allows a person exercising this power to remove

material from the premises where it is not reasonably practicable to determine if it is seizable to determine whether they are entitled to seize it at a later point. It also allows a person to seize material where it is not reasonably practicable to separate it from non-seizable material, for example where the seizable material is on a computer.

Information offences and penalties

Section 109: Offences in connection with information notices

549 This section sets out the criminal offences that can be committed in relation to information notices issued by OFCOM. It is an offence for such persons to:

a. fail to comply with OFCOM's information request;

b. provide false information to OFCOM in response to their information request;

c. provide encrypted information to OFCOM that it is not possible to understand in response to OFCOM's information request; and

d. suppress, destroy or alter information requested by OFCOM.

550 Subsection (7) provides that these offences may be committed only in relation to information notices which meet the conditions set out in paragraphs (a) and (b). Subsection (8) further provides for a subsequent court order to be made requiring compliance with an information notice where a person has been convicted of an offence.

Section 110: Senior managers' liability: information offences

551 This section sets out the criminal offences that can be committed by named senior managers in relation to their entity's information obligations. Senior managers who are named in a response to an information notice can be held criminally liable for failing to prevent the relevant service provider from committing an information offence.

552 Senior managers can only be prosecuted under this section where the regulated provider has already been found liable for failing to comply with OFCOM's information request.

Section 111: Offences in connection with notices under Schedule 12

553 This section establishes offences in connection with notices under Schedule 12. Subsection (2) provides that it is an offence, in connection with audit notices, for persons to fail to comply with a requirement of an audit notice without reasonable excuse. It is also an offence to knowingly provide false information in response to an audit notice.

554 Subsection (3) provides that it is an offence in connection with inspection or audit notices for a person to intentionally suppress, destroy or alter information required to be provided to OFCOM.

555 Upon conviction of an offence under this section, the court may, on the prosecutor's application, make an order requiring the convicted person to comply with a requirement of a notice under paragraph 3 of Schedule 12 or an audit notice.

Section 112: Other information offences

556 This section establishes additional information-related offences. It is a criminal offence for persons to:

a. intentionally obstruct or delay a person copying a document;

b. fail to attend or participate in an interview with OFCOM; and

c. knowingly or recklessly provide false information when being interviewed by OFCOM.

557 Upon conviction under this section, the court may require the convicted person to comply with making a copy of a document or a requirement in relation to interviews under section 96 within a specified period.

Section 113: Penalties for information offences

558 This section establishes penalties for various information offences contained in sections 109, 110, 111 and 112.

Disclosure of information

Section 114: Co-operation and disclosure of information: overseas regulators

559 This section grants OFCOM a power for collaboration and information sharing with an overseas regulator, including by disclosing online safety information in order to facilitate an overseas regulator exercising their online safety functions, or to cooperate with any related criminal investigations or proceedings. An overseas regulator is a person in a country outside the United Kingdom which exercises functions corresponding to OFCOM's online safety functions and the power only applies in relation to an overseas regulator specified in regulations made by the Secretary of State.

560 Under subsection (3), unless an overseas regulator has OFCOM's consent or is acting in accordance with an order of a court or tribunal, they cannot use the information disclosed under this power for another purpose, or disclose it further.

561 Subsection (4) provides that disclosure under this power does not breach any obligation of confidence owed by the person making the disclosure, or any other restriction on such disclosure, other than the exceptions specified in subsection (5).

562 Subsection (6) allows the Secretary of State to give a direction prohibiting the disclosure of information under this power for the purposes of overseas proceedings or overseas proceedings of any description specified in that direction.

Section 115: Disclosure of information

563 This section amends section 393 of the Communications Act 2003 (general restrictions on disclosure of information) to include new provisions under this Act. Section 393 provides that, subject to specific exceptions, information obtained by OFCOM in the exercise of their functions under the Communications Act 2003, Broadcasting Act 1990 and Broadcasting Act 1996 cannot be disclosed without the consent of the business in question.

564 Subsection (2) has the effect that, subject to the specific exceptions in section 393 of the Communications Act 2003, OFCOM cannot disclose information with respect to a business which they have obtained by exercising their powers under the Online Safety Act 2023 without the consent of the business in question.

565 Subsection (3) amends the list of exceptions in section 393(2) of the Communications Act 2003 so OFCOM can disclose information about a business, without its consent, for the purposes of any civil proceedings brought under the Online Safety Act 2023.

566 Subsections (4) and (5) amend the list of exemptions in section 393 of the Communications Act 2003 so as to allow OFCOM to disclose information obtained using its Online Safety Act powers about a business, without its consent, to a coroner or the procurator fiscal.

567 Subsection (6) has the effect that the section 393 Communications Act 2003 restriction on disclosure does not apply to details of enforcement action under section 127 or research or other information published under Schedule 8.

568 Similarly, subsection (7) ensures that section 393 of the Communications Act 2003 does not limit the matters that may be included in, or made public as part of, a report made by OFCOM under the Online Safety Act 2023.

Section 116: Intelligence service information

569 This section places a duty on OFCOM to consult the relevant intelligence service before OFCOM discloses or publishes any information they have received (directly or indirectly) from that intelligence service.

570 Subsection (1) sets out that OFCOM cannot disclose any information that they have received from an intelligence service, or information about an intelligence service, unless OFCOM have received consent from the intelligence service to disclose the information.

571 Subsection (2) states that if OFCOM discloses information as set out in subsection (1) to a person, then that person must not further disclose the information unless they have received consent from the intelligence service to do so.

572 Subsection (3) states that if OFCOM were to publish the documents set out in (a) and (b) which contain information set out in subsection (1), then OFCOM must remove or obscure the information that cannot be disclosed due to subsection (1) before the documents are published.

Section 117: Provision of information to the Secretary of State

573 The section makes amendments to section 24B of the Communications Act 2003 (CA 2003), which allows OFCOM to provide information to the Secretary of State that OFCOM considers may assist the Secretary of State in the formulation of policy.

574 Subsection (2) of this section amends section 24B(2) of the CA 2003 so that, where information relating to a particular business has been obtained using a power under the Online Safety Act 2023, OFCOM may not provide this information to the Secretary of State without the consent of the person carrying on that business whilst the business is carried on. This does not affect the fact that consent must still also be obtained for OFCOM to share information that has been acquired using powers in the CA 2003, the Broadcasting Act 1990, the Broadcasting Act 1996, the Wireless Telegraphy Act 2006 or Part 3 of the Postal Services Act 2011 (which were already listed in section 24B(2) of CA 2003).

575 Subsection (3) inserts a new subsection (3) into section 24B of the CA 2003. This new subsection provides that section 24B(2) does not apply, and therefore the consent of the person carrying on the relevant business is not required, for OFCOM to share information which is reasonably required by the Secretary of State and:

a. Was obtained by OFCOM using the power under section 100 in order to determine a proposed threshold figure, which if met or exceeded by providers renders them liable to pay fees to OFCOM (the purpose under subsection (5)(c) of that section); or

b. Was obtained by OFCOM using the power under section 175(5) to require information from a provider of a regulated service in response to potential threats to national security, or to the health or safety of the public.

Section 118: Amendment of Enterprise Act 2002

576 This section amends Schedule 15 of the Enterprise Act 2002 to enable the Competition and Markets Authority to share information with OFCOM to facilitate the exercise of OFCOM's functions under the Online Safety Act 2023.

577 This section adds the Online Safety Act 2023.3 to Schedule 15 of the Enterprise Act 2002 so that it is a 'specified enactment' for the purposes of section 241(3)(b) of the Enterprise Act 2002. This allows disclosure of certain kinds of information to OFCOM for the purposes of OFCOM's online safety functions.

Section 119: Information for users of regulated services

578 The section makes amendments to section 26 of the Communications Act 2003 (CA 2003) which provides for publication of information and advice for various persons, such as consumers.

Section 120: Admissibility of statements

579 Subsection (1) sets out the circumstances in which a statement given to OFCOM, in connection with OFCOM's power to require information under section 100, OFCOM's power to require interviews under section 106 or required under OFCOM's powers of entry and inspection under Schedule 12, may be used in evidence against the person who gave the statement.

Chapter 5: Regulated user-to-user services and regulated search services: notices to deal with terrorism content and CSEA content

Section 121: Notices to deal with terrorism content or CSEA content (or both)

580 Chapter 5 provides the statutory basis for OFCOM's power to require a service provider to use accredited technology to tackle terrorism content and child sexual exploitation and abuse (CSEA) content and/or develop and source technology to tackle CSEA content.

581 Subsection (1) sets out that OFCOM may issue a notice to a service provider of a regulated user-to-user service or a regulated search service, when doing so is necessary and proportionate.

582 Subsections (2)(a) states that OFCOM may require a service provider of a regulated user-to-user service to use accredited technology to identify terrorism content communicated publicly (as defined in section 237) and/or CSEA content on any part of the service. The service must take down that content without delay. The service may also be required to prevent this content from being made accessible to users at the outset, so that they do not encounter it, for example by preventing the content from being uploaded onto the platform.

583 Subsection (2)(b) states that OFCOM may require a service provider of a regulated user-to-user service to use its best endeavours to source or develop technology to identify and remove CSEA content on any part of the service or to prevent users from encountering this content. This technology must meet minimum standards of accuracy.

584 Subsection (3) states that OFCOM may issue a notice under this section to search services, and subsection (4) makes clear that any notice given under subsections (2) or (3) can be issued to a provider that has both user-to-user functions and search functions.

585 Subsection (5) states that in removing terrorism or CSEA content under subsections (2) and/or (3), providers may solely deploy accredited technology, or a combination of accredited technology and human moderators.

586 Subsection (6) refers to section 122, section 123, and section 124, which set out the process hat OFCOM must follow in issuing a notice to a service provider as set out in subsection (1) and states that OFCOM must issue a warning notice before issuing a notice under this section.

Section 122: Requirement to obtain a skilled person's report

587 This section states that OFCOM must obtain a skilled person's report under section 104 before issuing a notice to a provider.

Section 123: Warning notices

588 This section sets out the process that OFCOM must follow in issuing a warning notice.

589 Subsection (1) states that OFCOM may only issue a notice under section 121(1) to a service provider once they have given a warning notice.

590 Subsection (2) provides the details that OFCOM must include when issuing a warning notice to use accredited technology and subsection (3) provides the details that OFCOM must include when issuing a warning notice to develop or source technology. This includes a summary of the skilled person's report required by section 122.

591 Subsection (4) sets out the process that OFCOM must follow when issuing a warning notice for a combined user-to-user and search service.

592 Subsection (5) states that a notice can only be issued by OFCOM once the period in which a company can make representations, as set out in a warning notice, has finished.

Section 124: Matters relevant to a decision to give a notice under section 121(1)

593 This section sets out the circumstances under which OFCOM may issue a notice to a service provider, and the conditions that must be met before the power can be used.

594 Subsection (1) states that OFCOM may only issue a notice, as set out in 121(1), when it is necessary and proportionate, and this section provides information to aid this decision making.

595 Subsections (2) and (3a) sets out matters that OFCOM must take into account when deciding whether issuing a notice to use accredited technology or a notice to develop or source technology is necessary and proportionate.

Section 125: Notices under section 121(1): supplementary

596 Subsection (2) provides that where a service provider is already using technology on a voluntary basis, but this is not sufficiently effective, OFCOM can still intervene and require a service provider to use a more effective technology, or the same technology in a more effective way.

597 Subsections (3) and (4) specify that OFCOM can include in the notice a requirement for service providers to operate an effective procedure for users to challenge the removal of their content from the service.

598 Subsection (5) states that if OFCOM decides that it is necessary and proportionate to issue a notice following representations from the company, the company must make proportionate alterations to the regulated service to ensure that the specified technology is effective when implemented.

599 Subsections (6) and (7) set out the information that must be contained within a notice to use accredited technology and the period it may last for. OFCOM may specify the way in which the technology must be used on the service to effectively meet the aims of the notice and to meet the minimum standards of accuracy. This could include directions on how the technology should be implemented, including for example technical set up, human moderation requirements, or the image database to be used.

600 Subsection (8) sets out the information that must be contained within a notice relating to the development or sourcing of technology. This includes agreed steps that the provider must take in order to meet the requirement to make best endeavours to develop or source technology, the period of time in which these steps must be taken. Subsection (9) provides information that OFCOM must consider when deciding the time period for this.

601 Subsection (10) states that a notice may only impose requirements in relation to regulated services in the United Kingdom or regulated services that affect United Kingdom users.

602 Subsections (12) and (13) explain that OFCOM are only able to require the use of technologies, including those which have been developed or sourced in response to a notice, that have been assessed by either OFCOM, or a third party appointed by OFCOM, as meeting the minimum standards of accuracy for detecting terrorism and/or CSEA content as set out by the Secretary of State.

Section 126: Review and further notice under section 121(1)

603 Subsection (2) and (3) set out that under section 125(11), OFCOM also has the power to revoke the notice if there are reasonable grounds to believe that the provider is not complying with it. If a notice is revoked and the matters in section 124 are considered, OFCOM can issue a further notice.

604 Subsection (4) requires OFCOM to review whether a service provider has complied with a notice to use accredited technology before the end of the notice, and to review a notice to develop or source technology by the last date that any steps are required have been taken.

605 Subsection (5) specifies what OFCOM must consider in their review of a service provider's compliance with a notice to use accredited technology.

606 Subsection (6) specifies that following the review, and after consultation with the provider, OFCOM may give the provider a further notice if OFCOM consider that it is necessary and proportionate to do so, taking into account the matters set out in section 124. Subsections (8) and (9) make clear that OFCOM are not required to obtain a skilled person's report or issue a warning notice in relation to a further notice, and it may also impose different requirements than an earlier notice.

Section 127: OFCOM's guidance about functions under this Chapter

607 This section requires OFCOM to issue guidance setting out how it proposes to exercise its powers under section 121.

608 OFCOM will have the discretion to decide on the exact content of the guidance and must keep it under review and publish it. OFCOM must also have regard to their guidance when exercising these powers. Before preparing the guidance, OFCOM must consult the Information Commissioner.

Section 128: OFCOM's annual report

609 This section requires OFCOM to report annually to the Secretary of State on the exercise of its power under section 121 during the last year. This report must include details of current technology that meets minimum standards of accuracy, and technology that is in-development that is likely to meet these standards.

610 Subsection (2) says that the Secretary of State must lay this report before Parliament.

611 Subsection (3) cross-refers to section 164 which sets out provisions for OFCOM excluding confidential information from its published reports.

Section 129: Interpretation of the Chapter

612 This section sets out that the definitions of "search content" and "search results", "terrorism content" and "CSEA content" used in Chapter 5 are the same as those used in Part 3.

Chapter 6: Enforcement Powers

Provisional notices and confirmation decisions

Section 130: Provisional notice of contravention

613 This section addresses the process of starting enforcement. OFCOM must first issue a "provisional notice of contravention" to an entity before they reach their final decision about whether to issue a confirmation decision, including any specific steps the service will be required to take and/or any financial penalty that will be imposed as a result.

614 The provisional notice of contravention must be sent to the relevant entity or person. This notice sets out OFCOM's provisional decision that an entity has breached its duties, sets out how it has failed, or is failing, and the evidence OFCOM have of this. The notification must detail any proposed requirements that the person must take to comply with the duty or requirement, or remedy the contravention and/or the financial penalties OFCOM intend to impose.

615 Subsection (8) establishes a process for recipients of provisional notices to make representations to OFCOM, and provide evidence in response to the provisional findings set out in the notice. OFCOM's notice has to explain this process, and give a deadline for providing representations. This process means that OFCOM can only reach a final decision after allowing the recipient the chance to make representations.

Section 131: Requirements enforceable by OFCOM against providers of regulated services

616 This section lists the "enforceable requirements". Failure to comply with these enforceable requirements can trigger enforcement action.

617 The enforceable requirements include, for example, duties to carry out and report on risk assessments, safety duties (including specific duties relating to children) and duties related to users' rights (freedom of expression and privacy).

Section 132: Confirmation decisions

618 If, having followed the required process (see section 130), OFCOM's final decision is that a regulated service has breached an enforceable requirement, OFCOM will issue a confirmation decision. This will set out OFCOM's final decision and will explain whether OFCOM requires the recipient of the notice to take any specific steps and/or pay a financial penalty.

Section 133: Confirmation decisions: requirements to take steps

619 A confirmation decision may require a person to take specific steps to either come into compliance with their duties or remedy the breach that they have committed.

620 OFCOM must allow a reasonable period for the recipient to complete the required steps. However, subsection (5) provides that OFCOM can require immediate action when the recipient has breached its information duties (because it will already be on notice as to what is required).

621 Section 136 allows OFCOM to require services to use a particular kind of "proactive technology" in their confirmation decisions, with certain constraints and safeguards. Proactive technology is defined in section 231.

622 Subsection (3) says that requirements to take steps can only relate to the operation of a regulated service within the United Kingdom, or in so far as it affects United Kingdom users of the service.

623 Subsection (4) sets out certain details that must be included in a confirmation decision which requires specific steps to be taken. This includes the steps that are required, OFCOM's reasoning and the recipient's appeal rights.

624 Subsections (6) requires OFCOM to specify in a confirmation decision which requirements (if any) in that notice are CSEA requirements.

625 Subsection (7) provides that OFCOM must designate a step as a CSEA requirement where a confirmation decision imposes a requirement to take steps in relation to a failure to comply with specific illegal safety duties in respect of CSEA content or an offence under Schedule 6. Failure to comply with a CSEA requirement is an offence (see section 138).

Section 134: Confirmation decisions: risk assessments

626 This section applies where OFCOM have found that a regulated provider has failed to carry out an illegal content or children's risk assessment properly or at all; and have identified a risk of serious harm which the regulated provider is not effectively mitigating or managing.

627 In such cases OFCOM can require the regulated provider to comply with the parts of its illegal content safety duties or children's safety duties that require the provider to mitigate and manage that risk of harm as if it had been identified in the relevant risk assessment. The intention is that the provider will be required to mitigate the risk that OFCOM have identified despite the provider itself not having identified the risk in its risk assessment. OFCOM will specify the date by which the regulated provider must take or use measures to comply with the duty in question.

628 The requirement to take these measures will apply until the regulated provider has fully complied with the relevant risk assessment duties.

Section 135: Confirmation decisions: children's access assessments

629 This section applies where OFCOM have found that a regulated provider has failed to properly carry out a children's access assessment set out in section 36.

630 In such cases, OFCOM can require a regulated provider to carry out or re-do the children's access assessment and would set a deadline for the completion of the assessment in the confirmation decision. The maximum period of time OFCOM can allow the service to complete the assessment is three months from the date of the confirmation decision (although this can subsequently be extended at OFCOM's discretion).

631 This section also gives OFCOM the power to determine that a service is likely to be accessed by children where there is evidence that it is possible for children to access all or part of the service and the child user condition in section 35(3) is met. (The child user condition is met if either: (a) a significant number of children are users of the service, or part of the service; or (b) the service, or part of it, is likely to attract a significant number of child users). If OFCOM determine that a service is likely to be accessed by children, the children's risk assessment duties in section 28 and the children's safety duties in section 29 will apply to the service. OFCOM will specify the date from which the duties would apply in their confirmation decision. OFCOM can also set out the circumstances in which their determination will cease to apply in their confirmation decision.

Section 136: Confirmation decisions: proactive technology

632 This section sets out when OFCOM may, in a confirmation decision, require a service to use a kind of "proactive technology" specified in the confirmation decision.

633 Subsection 2(b)) sets out that OFCOM may require a provider to use proactive technology in a confirmation decision, if the purpose is to deal with non-compliance with section 81(2) (provider pornographic content).

634 The section also sets out the matters OFCOM must consider before deciding to impose such a requirement.

635 OFCOM may only require the use of proactive technology on content which is communicated publicly. Therefore, subsection (8) provides that a confirmation decision which requires the use of such technology must identify the content, or parts of the service that include content, which OFCOM considers is communicated publicly.

636 Subsection (9) provides that OFCOM may set the requirement for the regulated service to review their use of any technology imposed in response to a confirmation decision.

637 "Proactive technology" is defined in section 231.

Section 137: Confirmation decisions: penalties

638 This section allows OFCOM to impose financial penalties in their confirmation decision. These can be a single amount or a daily rate penalty if the failure is ongoing. Before imposing any financial penalty in their confirmation decision, OFCOM must set out the proposed amount(s) to the recipient in their provisional notice of contravention and allow the recipient the chance to make representations.

639 Certain details must be included in a confirmation decision which imposes a penalty. This includes OFCOM's reasons for imposing a penalty, the breaches that have attracted the penalty, a deadline for payment and the consequences of non-payment.

Section 138: Confirmation decisions: offences

640 This section creates a new offence of failure to comply with requirements of a confirmation decision that relate to specified duties to protect children's online safety without reasonable excuse. The specified duties are those at section 12(3)(a), section 12(3)(b), section 81(2), or section 81(4).

641 This section further provides that a person commits an offence if the person fails to comply, without reasonable excuse, with a CSEA requirement imposed by a confirmation decision given to the person.

642 A person who commits an offence under this section is liable for different penalties on summary conviction in England and Wales, Scotland and Northern Ireland, and to imprisonment for a term not exceeding 2 years or a fine (or both) on conviction on indictment.

Penalty notices etc

Section 139: Penalty for failure to comply with confirmation decision

643 This section allows OFCOM to impose a financial penalty on a person who fails to complete steps required by OFCOM in a confirmation decision. OFCOM can only impose a penalty under this section if they have not imposed a daily rate penalty in respect of the same failure in its confirmation decision (to prevent the person being penalised twice for the same delay).

Section 140: Penalty for failure to comply with notice under section 121(1)

644 This section allows OFCOM to impose a financial penalty on a person who fails to comply with a notice issued under section 109(1), which is a notice that requires technology to be implemented to identify and deal with terrorism content and/or CSEA content on a service.

Section 141: Non-payment of fee

645 Section 84 explains where OFCOM may require a provider of a regulated service to pay a fee. Schedule 10 also provides for fees to be charged to providers to enable OFCOM to recover costs they have incurred undertaking work which directly or indirectly prepares OFCOM for their future role as the online safety regulator. If a provider of a regulated service does not pay its fee, either under section 84 or Schedule 10, to OFCOM in full, OFCOM may give that provider a notice specifying the outstanding sum and the date by which it must be paid.

646 Section 142 allows OFCOM to give a penalty notice to a provider of a regulated service who does not pay the fee due to OFCOM in full. OFCOM may only impose such a penalty where they have first notified the provider that they propose to do so in a notice issued under this section and then given the provider the opportunity to make representations. OFCOM must also be satisfied that the unpaid fee is outstanding.

Section 142: Information to be included in notices under sections 140 and 141

647 This section requires OFCOM to include certain information in penalty notices issued under sections 140 and 141. For example, OFCOM must state the reasons why they are imposing a penalty, the amount of the penalty and any aggravating or mitigating factors. OFCOM must also state when the penalty must be paid.

Amount of penalties etc

Section 143: Amount of penalties etc

648 This section cross-refers to Schedule 13 which sets out details on the financial penalties that OFCOM may impose under this Act, including the maximum amount that may be imposed. OFCOM are required to produce guidelines setting out how they determine penalty amounts.

Schedule 13: Penalties imposed by OFCOM under Chapter 6 of Part 7

Amount of penalties: principles

649 Paragraph 2 of Schedule 13 sets out the things that OFCOM must take into account when determining the size of the penalty. This includes any representations made by the person or evidence provided by the person and the effects of the failure. OFCOM must also consider any steps taken by the person to comply with the requirements set out in the provisional notice,

confirmation decision or penalty notice, and any steps taken to remedy the failure. Any penalty that OFCOM imposes must be considered by OFCOM to be appropriate and proportionate to the failure (or failures).

Limitation to type and amount of penalties previously proposed

650 Paragraph 3 of Schedule 13 confirms that a penalty imposed by a confirmation decision or penalty notice may not exceed the amount of the penalty, or (if relevant) be payable over a longer period than was proposed in the earlier notice about the same breach(es).

651 However, the limiting impact of earlier notices on subsequent penalties, as set out in paragraph 3 of Schedule 13, does not apply in relation to a penalty for which two or more entities are jointly and severally liable for the breach(es) (see paragraph 3(2)), unless the provisional notice and confirmation decision is given jointly (see Schedule 15).

Maximum amount of penalties

652 Paragraph 4(1) of Schedule 13 says that the maximum penalty that OFCOM can impose on the provider of a regulated service is the greater of £18 million and 10% of the person's "qualifying worldwide revenue" for the person's most recent complete accounting period.

653 Paragraphs 4(4)-(6) also includes further detail on how "qualifying worldwide revenue" will be calculated. The term "qualifying worldwide revenue" will be defined in a statement produced and published by OFCOM under section 76.

Maximum amount of penalties: group of entities

654 Schedule 15 sets out the circumstances when OFCOM may hold two or more entities jointly and severally liable for a breach. Paragraph 5 of Schedule 13 sets out how penalties are to be calculated in such a scenario.

655 Paragraph 5(3) states that the maximum penalty that OFCOM can impose in such cases is the greater of £18 million and 10% of the "qualifying worldwide revenue" of the group of entities of which the provider of the regulated service is a member.

656 Paragraph 5(4) defines the "qualifying worldwide revenue" for a group of entities.

657 "Qualifying worldwide revenue" will be set out in a statement produced and published by OFCOM under section 86. The statement must include provision about the application of that term to a group of entities.

Recovery of penalties

658 Paragraph 6 of Schedule 13 sets out how payment of penalties can be recovered and enforced.

Business disruption measures

Section 144: Service restriction orders

659 The Act gives OFCOM the power to apply to the courts for "business disruption measures". Business disruption measures are court orders that require third parties to withdraw services or block access to non-compliant regulated services. They are designed to only be used for the most serious instances of user harm. There are two types of business disruption measures: "service restriction orders" and "access restriction orders". The details and grounds for both are covered in sections 144 to 148.

660 Section 144 sets out the circumstances in which OFCOM may apply to the court for a "service restriction order". Service restriction orders are orders that require providers of "ancillary services" (persons providing, for example, payment or advertising services) to take steps aimed at disrupting the business or revenue of a non-compliant provider's operations in the United Kingdom. For example, an order could require an advertising service to cease the provision of its service to a non-compliant provider's service.

Section 145: Interim service restriction orders

661 This section sets out the circumstances in which OFCOM may apply to the courts for an "interim service restriction order". OFCOM can apply for an interim service restriction order in circumstances where it is not appropriate to wait for a failure to comply with an enforceable requirement to be established before making the order. OFCOM are not required to demonstrate to the court that a failure has been established (something which can take a long time), but must demonstrate that it is likely that the provider is failing to comply with a requirement under the Act, and that the nature and severity of that harm mean that it would not be appropriate to wait to establish the failure before applying for the order.

662 An interim service restriction order will cease to have effect on the earlier of either the date specified in the order, or the date on which the court makes a service restriction order under section 144 that imposes requirements on the persons who are subject to the interim service restriction order (or dismisses the application for such an order).

Section 146: Access restriction orders

663 This section sets out the circumstances in which OFCOM may apply to the courts for an "access restriction order". An access restriction order can require third parties who provide an "access facility" to take steps to impede access to a non-compliant regulated service, by preventing, restricting or deterring individuals in the United Kingdom from accessing that service. Examples of access facilities are internet service providers and app stores which may be required to restrict access to a service provider's website or app via their service.

664 In order to apply for an access restriction order, OFCOM must consider that a service restriction order under section 144 or 145 would not be sufficient to prevent significant harm to individuals in the United Kingdom.

Section 147: Interim access restriction orders

665 This section sets out the circumstances in which OFCOM may apply to the courts for an interim access restriction order. OFCOM can apply for an interim access restriction order in those circumstances where it is not appropriate to wait for the failure to be established before making the order (for example, if there is serious user harm that requires quick action to impede access). OFCOM are not required to demonstrate to the court that a failure has been established (something which can take a long time), but must demonstrate that certain conditions exist which mean that it would not be appropriate to wait to establish the failure before applying for the order.

Section 148: Interaction with other action by OFCOM

666 This section explains how business disruption orders interact with OFCOM's other enforcement powers. Where OFCOM exercise their powers to apply to the courts for business disruption orders under sections 144 to 147, they are not precluded from taking action under their other enforcement powers.

Publication of enforcement action

Section 149: Publication by OFCOM of details of enforcement action

667 If, having followed the required process (see section 130), OFCOM's final decision is that a regulated service has breached an enforceable requirement, OFCOM will issue a confirmation decision under section 132. This will set out OFCOM's final decision and will explain whether OFCOM require the recipient of the notice to take any specific steps and/or pay a financial penalty.

668 Where OFCOM issue a confirmation decision, they are obliged to publish the identity of the person to whom the confirmation decision was sent, details of the failure to which the confirmation decision relates and details relating to OFCOM's response.

669 OFCOM are also obliged to publish these details when they give a person a penalty notice for: failing to comply with a confirmation decision (under section 139); failing to comply with a notice to deal with terrorism content or CSEA content (or both) (under section 140(5)); and failing to pay a fee in full (under section 141(6)).

670 This is intended to provide transparency in relation to OFCOM's enforcement activities.

Section 150: Publication by providers of details of enforcement action

671 This section gives OFCOM a power to require regulated services to publish the details, or otherwise notify UK users, of OFCOM's enforcement action. When using this power OFCOM must set out in a publication notice what enforcement decision or notice it is referring to, the detail that is to be published or notified, the form and manner in which it must be published or notified, the date by which is must be published or notified, as well as information about the consequences of not complying with the publication requirement.

672 This measure is intended to promote transparency by increasing awareness amongst users about providers' breaches of duties in the Act.

Guidance

Section 151: OFCOM's guidance about enforcement action

673 This section requires OFCOM to publish guidance about how they will use their enforcement powers. This is intended to help regulated providers and other stakeholders understand how OFCOM will exercise their enforcement powers.

Chapter 7: Committees, research and reports

Section 152: Advisory committee on disinformation and misinformation

674 This section places an obligation on OFCOM to form an advisory committee on disinformation and misinformation. This is because the spread of inaccurate information, regardless of intent, is particularly concerning. The section sets out what OFCOM should consider when appointing committee members, what the functions of the committee are, and what the committee's reporting obligations are.

Section 153: Functions of the Content Board

675 The Content Board is a committee of the main OFCOM Board, with delegated and advisory responsibilities. This section amends section 13 of the Communications Act 2003 (functions of the Content Board) to clarify that it allows, but does not require, OFCOM to confer functions on the Content Board in relation to OFCOM's content related functions under the Online Safety Act 2023.

Section 154: Research about users' experiences of regulated services

676 This section amends section 14 of the Communications Act 2003 (consumer research) to require OFCOM to arrange research into United Kingdom users' opinions and experiences relating to regulated services.

677 Subsection (2) provides that OFCOM must make arrangements to understand a number of factors, including public opinion concerning providers of regulated services and the experiences and interests of those using regulated services. The intention is to provide OFCOM with the flexibility to choose the most appropriate methods for such research. This subsection also provides that OFCOM must include a statement of the research they have carried out in their annual report to the Secretary of State and the devolved administrations, under paragraph 12 of the Schedule to the Office of Communications Act 2002.

Section 155: Consumer consultation

678 This section extends the Consumer Panel's remit to include online safety by amending section 16 of the Communications Act 2003 (consumer consultation).

679 It ensures that the Consumer Panel is able to give advice on matters relating to different types of online content (under this Act) and the impacts of online content on United Kingdom users of regulated services.

Section 156: OFCOM's statement about freedom of expression and privacy

680 This section requires OFCOM to publish annual reports on the steps they have taken when carrying out online safety functions to uphold users' rights under Articles 8 and 10 of the Convention, as required by section 6 of the Human Rights Act 1998.

Section 157: OFCOM's report about use of age assurance

681 This section requires OFCOM to produce and publish a report about the use of age assurance by providers of regulated services.

682 Subsections (1) and (2) specify that the report should assess how providers of regulated services have used age assurance to comply with their duties, how effective the use of age assurance has been for that purpose, and whether there are factors that have prevented or hindered the effective use of age assurance for that purpose. The report must pay particular consideration to whether the costs to providers of using age assurance, or the need to protect users' privacy, have prevented or hindered the effective use of age assurance.

683 Subsection (3) specifies that OFCOM must publish one report within the period of 18 months beginning with the day on which sections 12 and 81(2) come into force, unless the Secretary of State requires the production of a further report, as set out in subsubsection (6).

684 Subsections (4) and (5) set out consultation and procedural requirements.

685 Subsections (6) and (7) provide that the Secretary of State may require OFCOM to produce and publish a further report in response to developments in age assurance technologies or evidence of the reduced effectiveness of such technologies. This cannot be required until at least three years after the date on which the first report is published, or more frequently than once every three years.

Section 158: OFCOM's reports about news publisher content and journalistic content

686 This section requires OFCOM to publish a report about how the Act's regulatory framework impacts on how news publisher and journalistic content is treated and made available by Category 1 services.

687 Subsection (1) specifies that the report should assess the impact of the regulatory framework on the availability and treatment of news publisher and journalistic content on Category 1 services.

688 Subsection (2) specifies that the report must be published within two years of the duties to protect news publisher content and journalistic content coming into force.

689 Subsection (3) specifies that the report must in particular pay attention to how effective the duties on Category 1 services to protect such content are.

690 Subsection (4) provides further detail on who OFCOM must consult when producing the report.

691 Subsection (5) specifies that OFCOM are required to send a copy of the report to the Secretary of State, who must lay it before Parliament.

692 Subsections (6) and (7) specify that the Secretary of State may require OFCOM to produce and publish further reports following the publication of the first report.

Section 159: OFCOM's transparency reports

693 This section creates a duty on OFCOM to produce their own reports based on information from the transparency reports that certain providers are required to publish. The intention is for the report to highlight key insights from the providers' reports, giving users a better understanding of the steps service providers are taking. The report must be published annually.

Section 160: OFCOM's report about reporting and complaints procedures

694 This section requires OFCOM to produce a report about the content reporting and complaints procedures operated by providers of Part 3 services.

695 OFCOM's report needs to take into account the experiences of users and others in reporting content and making complaints to providers of Part 3 services. OFCOM are required to specifically advise whether they consider that regulations ought to be made placing a duty on Category 1 services to offer alternative dispute resolution procedures (see section 217), and are able to make other recommendations that they consider would deliver better outcomes in relation to reports or complaints.

Section 161: OFCOM's report about use of app stores by children

696 This section requires OFCOM to produce a report about the use of app stores by children, including consideration of whether children would be better protected by greater use of age assurance on app stores. OFCOM are required to publish the report between 2 and 3 years following the commencement of the child safety duties.

Section 162: OFCOM's report about researchers' access to information

697 This section requires OFCOM to publish a report about the ability of independent researchers into online safety matters (as defined in section 235) obtain relevant information from providers of regulated services. The section sets out what OFCOM's report must cover and requirements around consultation, parliamentary procedure and publication. The report must be published within 18 months of the section coming into force. OFCOM must also publish guidance for researchers and independent regulators about the matters dealt with by the report.

Section 163: OFCOM's report in connection with investigation into a death

698 This section provides that OFCOM may produce a report dealing with any matters that they consider may be relevant in connection with a person's death, if the coroner gives OFCOM a notice or, in Scotland, the procurator fiscal requests information for that purpose.

Section 164: OFCOM's reports

699 This section gives OFCOM a discretionary power to publish reports about certain specified online safety matters. OFCOM must have regard to the need to consider excluding confidential matters from their reports to the extent it is practicable. An example of this might be information that is commercially sensitive.

Chapter 8: Media Literacy

Section 165: Media literacy

700 This section introduces new objectives that OFCOM are required to achieve in fulfilment of its current duty to promote media literacy under section 11 of the Communications Act 2003, insofar as it relates to regulated services. The first of these new duties requires OFCOM to bring about better public awareness and understanding of ways in which they may keep themselves and others safe whilst using regulated services, with particular emphasis on six new objectives. The second duty requires OFCOM to encourage the development and use of technologies and systems that support users of regulated services to protect themselves and others online. To achieve the new objectives, and fulfil the first duty more broadly, OFCOM are required to pursue, commission, and encourage other organisations to pursue media literacy initiatives and arrange for research to be carried out. This section also requires OFCOM to publish and occasionally update a set of recommendations for how organisations delivering media literacy initiatives, including regulated services, can do so more effectively.

Section 166: Media literacy strategy and media literacy statement

701 This section requires OFCOM to publish a media literacy strategy within one year of the Act receiving Royal Assent. A media literacy strategy needs to cover a maximum of three years and before the end of this period OFCOM are required to prepare and publish a new media literacy strategy. The strategy needs to state OFCOM's objectives and priorities for the period it covers. This section also requires OFCOM to publish a media literacy statement within its annual report, which needs to include a summary of the activities and initiatives delivered under section 11 of the Communications Act 2003.

Part 8: Appeals and super-complaints

Chapter 1: Appeals

Section 167: Appeals against OFCOM decisions relating to the register under section 95

702 This section allows for appeals against OFCOM's decisions to include, or not to remove, services from OFCOM's register of Category 1, Category 2A, and Category 2B services. Service providers who are registered by OFCOM as Category 1, Category 2A, and Category 2B services become subject to additional duties under the Act.

703 Appeals may be made by regulated providers to the Upper Tribunal. The Upper Tribunal must apply the same principles as a court would when hearing an application for judicial review. The section also provides that where a regulated provider has filed an appeal, any additional

duties or requirements applying under the Act associated with that provider being designated as a Category 1, 2A, or 2B operator need not be complied with until the determination or withdrawal of the appeal.

704 The Upper Tribunal may either dismiss the provider's appeal or quash OFCOM's decision. Should the Tribunal quash the decision then the Tribunal must remit the decision back to OFCOM.

Section 168: Appeals against OFCOM notices

705 This section allows for appeals against decisions by OFCOM to issue a confirmation decision, a notice under section 121(1) or a penalty notice. An appeal may be brought to the Upper Tribunal by any person with sufficient interest in the decision, although anyone other than the recipient requires permission from the Upper Tribunal to appeal.

706 The Tribunal will apply the same principles as a court would when hearing an application for judicial review.

707 The Upper Tribunal may either dismiss the appeal or quash OFCOM's decision. Should the Tribunal quash the decision then the Tribunal must remit the decision back to OFCOM for reconsideration, with any directions that the Tribunal thinks are appropriate.

Chapter 2: Super-complaints

Section 169: Power to make super-complaints

708 This section establishes a super-complaints mechanism which enables any organisation or other entity that meets the relevant eligibility criteria to bring systemic issues to OFCOM in specific circumstances.

709 A super-complaint can be about any feature of a regulated service or conduct of the provider of such a service. It may relate to one or more regulated services or providers and may be about any combination of features and conduct. Where this feature, conduct or combination of the two is causing, appears to be causing or is at material risk of causing users or members of the public significant harm, significantly adversely affecting their right to freedom of expression, or having a significant adverse impact on them, an eligible entity may make a super-complaint.

710 Where a super-complaint relates to the conduct of a single regulated service or single provider of one or more regulated services, OFCOM may only consider it if they believe that the complaint is of particular importance or it relates to impacts on a particularly large number of people.

Section 170: Procedure for super-complaints

711 This section requires the Secretary of State to make regulations which set out the procedural aspects of complaints made under section 169. It provides examples of the matters that these regulations may include provision for; for example, pre-notifying OFCOM of an organisation's intention to make a super-complaint.

712 The Secretary of State must consult OFCOM and anyone else they consider to be appropriate before making these regulations.

Section 171: OFCOM's guidance about super-complaints

713 This section puts a requirement on OFCOM to produce and publish guidance on super-complaints and sets out what the guidance must include.

Part 9: Secretary of State's functions in relation to regulated services

Strategic Priorities

Section 172: Statement of strategic priorities

714 This section introduces a power for the Secretary of State to set out a statement of the Government's strategic priorities in relation to online safety matters. This power is similar to the existing power the Secretary of State has in the Communications Act 2003 in relation to telecommunications, management of radio spectrum and postal services.

715 Before designating the statement, the Secretary of State must first consult and follow the parliamentary procedure set out in section 173.

716 The statement may specify particular outcomes to be achieved with a view to delivering the strategic priorities. For example, the Secretary of State may set a target eradication rate for child sexual exploitation and abuse (CSEA) images online or look to reduce regulatory burdens on service providers.

717 If a statement of strategic priorities is to be amended in whole or in part, this must be done by issuing a subsequent statement following the procedure in section 173. There are limited circumstances in which amendments may be made within a five year period, for example where there has been a significant change in government policy affecting online safety matters.

Section 173: Consultation and parliamentary procedure

718 This section sets out the consultation and parliamentary procedure requirements that must be satisfied before the Secretary of State can designate a statement of strategic priorities under section 172.

719 The Secretary of State must consult OFCOM and other persons the Secretary of State considers appropriate on a draft of the statement. For example, the Secretary of State may wish to consult other government departments, industry bodies, academics, policy institutes/think-tanks, or other regulators.

720 Subsection (3) provides for a period of at least 40 days for such consultation with OFCOM, following which the Secretary of State must make any changes to the draft statement that appear necessary to the Secretary of State. They must then lay the draft statement before Parliament (subsection (4)) where it is subject to the negative resolution procedure as set out in subsections (5) - (7). After that procedure the Secretary of State may designate the statement.

Directions to OFCOM

Section 174: Directions about advisory committees

721 This section enables the Secretary of State to give OFCOM a direction to establish an expert committee to advise OFCOM on a specific online safety matter. By way of example, a direction could be issued requiring OFCOM to establish a committee to provide advice on an emerging online safety issue. The committee could do this by facilitating multi-stakeholder dialogue and building a greater understanding of the respective issue.

722 Subsection (3) sets out that OFCOM must appoint a committee chair, and that the number of additional members is at OFCOM's discretion unless the direction specifies otherwise in either case.

723 Subsection (4) places a duty on an advisory committee established under this direction to publish a report within 18 months of it being established, unless the direction specifies otherwise. After the initial report, the committee is required to publish reports periodically at their own discretion.

Section 175: Directions in special circumstances

724 This section enables the Secretary of State to give OFCOM directions in circumstances where they consider there is a threat to the health or safety of the public, or to national security. This includes directing OFCOM to prioritise action to respond to a specific threat when exercising its media literacy functions and to require specified service providers, or providers of regulated services generally, to publicly report on what steps it is taking to respond to that threat. For example, the Secretary of State could issue a direction during a pandemic to require OFCOM to give priority to ensuring that health misinformation and disinformation is effectively tackled when exercising its media literacy function and to require service providers to report on the action they are taking to address this issue.

725 Subsection (6) specifies that the Secretary of State must publish the reasons for giving a direction in circumstances where this is given in response to a threat to the health or safety of the public. There is no requirement to publish reasons for giving a direction where this is done in response to a threat to national security.

726 The Secretary of State can vary or revoke a direction at any time. If so, OFCOM can vary or revoke the public statement notice they have given pursuant to the Secretary of State's direction: see subsection (7) and (8).

Guidance

Section 176: Secretary of State's guidance

727 This section enables the Secretary of State to give guidance to OFCOM relating to OFCOM's exercise of their statutory powers and functions under the Act. The guidance will provide clarity to OFCOM and others about how the Secretary of State expects OFCOM to carry out their statutory functions.

728 Subsections (3) to (7) detail the requirements for producing guidance issued under this section.

729 OFCOM must have regard to the guidance when exercising any functions to which the guidance relates or when considering whether or not to exercise such functions.

Annual Report

Section 177: Annual report on the Secretary of State's functions

730 Section 390 of the Communications Act 2003 requires the Secretary of State to prepare and lay before Parliament annual reports about their performance of the Secretary of State's functions under specific legislation, including the Communications Act 2003, the Office of Communications Act 2002 and the Broadcasting Acts 1990 and 1996.

731 This section amends the Communications Act 2003 by adding the functions under the Online Safety Act 2023 to the list of functions which the Secretary of State must include in their annual report to Parliament.

Review

Section 178: Review

732 This section provides for a review to be undertaken by the Secretary of State, published and laid before Parliament, between 2 and 5 years after the duties on services in Part 3 are commenced, in order to assess the effectiveness of the regulatory framework. The timing requirement is designed to ensure there is adequate time to allow the regime to be in operation before the review takes place, and that a review will take place in a timely manner.

733 The review must consider a number of areas in assessing the effectiveness of the regulatory framework. These areas include how effective the regulatory regime has been at ensuring that regulated services are operating, using systems and processes that minimise the risk of harm to individuals in the United Kingdom, and in providing higher levels of protection for children than for adults.

734 The Secretary of State is also required to take into account OFCOM's reports published under section 158.

735 The review must also consider the effectiveness of: OFCOM's information gathering, information sharing and enforcement powers; and the extent to which OFCOM have had regard to the desirability of encouraging innovation.

Part 10: Communications offences

False and threatening communications offences

Section 179: False communications offence

736 This section creates a criminal offence for the sending of false communications that meet the threshold of the offence. A person is guilty of the offence if, without reasonable excuse, they send a message conveying information that they know to be false, and at the time of sending it they intend the message to cause non-trivial psychological or physical harm to a likely audience - i.e. someone who could reasonably be foreseen to encounter the message or its content.

737 The prosecution must prove that the sender lacked a reasonable excuse for sending the message.

738 Subsection 5(a) sets out penalties for the false communications offence in England and Wales, and 5(b) sets out the penalties for the false communications offence in Northern Ireland. Subsection (6) sets out the definition of 'maximum term for summary offences' as referenced in subsection (5).

739 This offence replaces the offence in section 1(a)(iii) of the Malicious Communications Act 1988 and (for England and Wales and Northern Ireland) the offence in section 127(2)(a) and (b) of the Communications Act 2003. The relevant repeals are made by section 189 of the Act.

Section 180: Exemptions from offence under section 179

740 This section sets out exemptions for the false communications offence, including an exemption for recognised news publishers and limited exemptions for holders of broadcast or multiplex licences, providers of an on-demand programming service and holders of multiplex licences. This section also provides that the offence cannot be committed in connection with the showing of a film made for cinema to members of the public.

Section 181: Threatening communications offence

741 This section creates a criminal offence for the sending of threatening communications that meet the threshold in the offence. A section person who sends a message conveying a threat of death, serious injury, rape, assault by penetration, or serious financial loss, and intends that (or is reckless as to whether) someone encountering the message will fear the threat will be carried out, is guilty of the offence.

742 Subsection (1)(c)(i) and (1)(c)(ii) make it clear that the threatening communications offence captures threats where the recipient fears that someone other than the sender of the message may carry out the threat. This does not change the scope of this offence, which, like other existing offences to do with threats, would anyway capture threats carried out by third parties.

743 With respect to threats of serious financial loss, it is a defence for a sender to show both that the threat was used to reinforce a reasonable demand and that they reasonably believed the threat was a proper means of reinforcing the demand.

744 Subsection (5) sets out the penalties for this offence.

745 This offence replaces the offence in section 1(1)(a)(ii) of the Malicious Communications Act 1988, which is repealed by section 189 of the Act.

Section 182: Interpretation of sections 179 to 181

746 This section sets out how different aspects of the offences in sections 179 and 181 should be interpreted.

747 Subsection (2) and (3) makes provision about the interpretation of the phrase "sends a message."

748 Subsection (4) sets out that a provider of an internet service by which a message is sent is not to be regarded as a person who sends a message simply by virtue of providing that internet service.

749 Subsection (5) sets out the meaning of "encounter" in relation to a message.

750 Subsection (6) sets out that for the purposes of the offences it does not matter if the content of the message is created by the person who sends it. Subsection (7) sets out that a message can consist of or include a hyperlink to other content.

751 Subsection (8) deals with the sending or giving of items on which data is stored electronically.

752 Subsection (9) clarifies the timing of offences committed in the online context.

753 Subsections (10), (11) and (12) point to definitions of relevant terms in other Acts or elsewhere in the Act.

Offences of sending or showing flashing images

Section 183: Offences of sending or showing flashing images electronically

754 This section creates two specific offences of sending or showing flashing images electronically to people with epilepsy intending to cause them harm. "Harm" means a seizure, or alarm or distress (subsection (13)).

755 Subsection (1) creates an offence of sending a communication by electronic means which consists of or includes flashing images, where one of two conditions set out in either subsection (2) or subsection (3) are met, without a reasonable excuse.

756 The condition set out in subsection (2) - condition 1 - is that, at the time the communication is sent, it is reasonably foreseeable that an individual with epilepsy would be among the individuals who would view the communication, and the communication is sent with the intention that such an individual will suffer harm as a result of viewing the flashing images. Condition 1 is intended to capture speculative messages sent to multiple people, for example on social media.

757 The condition set out in subsection (3) - condition 2 - is that, when sending the communication, the person sending it believes that an individual whom the sender knows or suspects to be an individual with epilepsy will, or might, view it and intends that individual to suffer harm as a result of viewing the flashing images. Condition 2 is intended to capture the more targeted sending of flashing images to an individual who the sender knows, or suspects, has epilepsy.

758 Subsection (4) provides that references in subsections (2)(a) and (3)(a) to viewing the communication include references to viewing a subsequent communication forwarding or sharing the content of the communication. The offence in subsection (1) may therefore be committed by a person who forwards or shares the electronic communication, as well as by the person sending it.

759 Subsection (5) provides that the exemptions contained in section 161 also apply to an offence under subsection (1). This means that an offence of sending flashing images electronically cannot be committed: by recognised news publishers; by those with licences under the Broadcasting Acts 1990 or 1996; by the holder of a multiplex licence; by the providers of on-demand programme services; or in connection with the showing to members of the public of a film that was made for cinema.

760 Subsection (8) creates an offence of showing another person flashing images by means of an electronic communications device. The offence is committed if a person shows an individual flashing images, for example on a mobile phone screen, when showing the images knows or suspects that the individual concerned is an individual with epilepsy, intends that that individual will suffer harm as a result of viewing them, and if the person has no reasonable excuse for showing the images.

761 Subsection (9) provides an exemption for healthcare professionals acting in that capacity.

762 Subsection (10) provides that a person who commits an offence under subsection (1) or (8) is liable: on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court or a fine (or both); on summary conviction in Northern Ireland, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum (or both); and on conviction on indictment, to imprisonment for a term not exceeding five years or a fine (or both).

763 Subsection (11) provides that it does not matter whether images may be viewed immediately or only after some action, such as pressing play, is performed.

764 Subsection (12) provides that references to sending a communication or showing flashing images include references to causing a communication to be sent or causing flashing images to be shown.

765 Subsection (13) provides further definitions for the purposes of the section.

Offence of encouraging or assisting serious self-harm

Section 184: Offence of encouraging or assisting serious self-harm

766 This section outlines the offence of encouraging or assisting the serious self-harm of another person.

767 Subsection (1) provides that a person commits an offence if they do a relevant act capable of encouraging or assisting the serious self-harm of another person; and their act was intended to encourage or assist the serious self-harm of another person. Subsection (2) defines the means of communication by which a person "does a relevant act", which includes in-person or electronic communications, publications, correspondence, and the sending or giving of items with stored electronic data.

768 Subsection (3) provides that "serious self-harm" means self-harm amounting to, in England and Wales and Northern Ireland, grievous bodily harm within the meaning of the Offences Against the Person Act 1861 and, in Scotland, severe injury; and includes successive acts of self-harm which cumulatively reach that threshold.

769 Subsection (4) provides that the person committing the offence need not know, or even be able to identify, the person or persons who receive the communication. So, a person who intends that a recipient or recipients of their communication will seriously harm themselves is guilty of an offence, even though he or she may never know the identity of those who receive the communication. Subsection (5) provides that an offence can be committed whether or not serious self-harm occurs.

770 Subsection (6) provides that a person who arranges for someone else to do an act capable of encouraging or assisting the serious self-harm of another person will also be committing an offence if the other person does that act.

771 Subsection (7) provides that a person commits an offence under subsection (1) even if the content of their communication or publication was not created by them. For example, the offence may be committed online where someone forwards another person's direct message or shares another person's post, and it will also be committed where a person publishes a physical document such as a pamphlet or booklet even if they did not write the material.

772 Subsection (8) provides that where a communication is sent, transmitted or published by electronic means and it includes a hyperlink to other content, the reference in subsection (2)(b) to a communication includes content accessed directly via the hyperlink.

773 Subsection (9) provides that where a person sends, gives or makes available (i.e. places somewhere for a person to find) an item on which data is stored electronically the reference to the item in subsection (2)(f) includes content accessed by means of the item to which the recipient is specifically directed by the person sending, giving or making that item available. So, for example, if someone sends a person a memory stick containing material that is intended to encourage or assist them to seriously self-harm, they will commit an offence.

774 Subsection (10) provides that an internet service provider does not commit the offence merely for providing a means through which others can publish content that is capable of encouraging or assisting serious self-harm.

775 Subsection (11) clarifies that references to doing an act capable of encouraging or assisting the serious self-harm of another person include a reference to doing so by threatening another person or otherwise putting pressure on another person to seriously self-harm.

776 Subsection (12) provides that an act capable of encouraging or assisting the serious self-harm of another person includes a course of conduct.

777 Subsection (13) provides that an "act" of self-harm in subsection (3) includes an omission. So, for example, a person who encourages another person not to eat, not to drink or not to take required prescription medication would be captured by the offence.

778 Subsection (14) provides that a person who commits the offence is liable: on summary conviction in England and Wales, to a term not exceeding the general limit in a magistrates' court or a fine (or both); on summary conviction in Scotland, to a term not exceeding 12 months or a fine not exceeding the statutory maximum (or both); on summary conviction in Northern Ireland, to a term not exceeding six months or a fine not exceeding the statutory maximum (or both); and on conviction on indictment to a term not exceeding five years or a fine (or both).

Further provision

Section 185: Extra-territorial application and jurisdiction

779 Subsections (1) and (2) of this section provide that the offences established by sections 179(1) (false communications), 181(1) (threatening communications) and 183(1) (sending or showing flashing images) can be committed outside the United Kingdom, but only by an individual who habitually resides in England, Wales or Northern Ireland, or by a body incorporated or constituted under the law of England, Wales or Northern Ireland.

780 Subsections (3) and (4) set out that the offence established by section 184(1) (encouraging or assisting serious self harm) can be committed outside of the United Kingdom, but only if the act is done by an individual who is habitually resident in the United Kingdom, or a body incorporated under the law of any part of the United Kingdom.

781 Subsection (5) provides for courts in England and Wales and Northern Ireland to have jurisdiction over an offence under sections 179, 181 or 183 that is committed outside the United Kingdom.

782 Subsections (6) provides for courts in the United Kingdom to have jurisdiction over an offence committed under section 184 that is committed outside the United Kingdom. Subsection (7) makes specific provision for such proceedings being taken in Scotland.

Section 186: Liability of corporate officers

783 Subsections (1) and (2) establish that an officer of a body corporate can, where appropriate tests are met, be held criminally liable when the body corporate commits an offence under sections 179, 181, 183 or 184. An "officer", as defined in subsection (2) means a director, manager, associate, secretary or other similar officer; or a person purporting to act in any such capacity.

784 Subsections (3) and (4) make equivalent provision for the liability of partners when a Scottish partnership commits an offence under section 184. Subsection (4) extends the definition of "partner" to include someone purporting to act as a partner.

Offence to be inserted into Sexual Offences Act 2003

Section 187: Sending etc photograph or film of genitals

785 This section creates a new offence of sending etc a photograph or film of a person's genitals to another person, in England and Wales. It inserts a new section 66A into the Sexual Offences Act 2003 ("the 2003 Act"). Section 66A(1) provides that where a person (A) intentionally sends or gives a photograph or film of any person's genitals to another person (B), and either

A intends that B will see the genitals and be caused alarm, distress or humiliation, or A sends or gives the photograph or film for the purpose of obtaining sexual gratification and is reckless as to whether B will be caused alarm, distress or humiliation, A commits an offence.

786 Subsection (2) makes clear that "sending or giving" a photograph or film includes, in particular, sending it to another person by any means, electronically or otherwise, showing it to another person, and placing it for a particular person to find.

787 Subsections (3) to (5) set out what is meant by "photograph" and "film". In particular, subsection (5) makes clear that references to the terms include an image, whether made by computer graphics or in any other way, which appears to be a photograph or film; a copy of such an image, photograph, or film, and data stored by any means which is capable of conversion into such an image; photograph, or film.

788 Subsection (6) provides that the offence is triable either way. Following summary conviction, the maximum penalty is six month's imprisonment prior to the coming into force of paragraph 24(A) of Schedule 22 to the Sentencing Act 2020 upon and twelve months' thereafter. (Paragraph 24(A) of Schedule 22 to the Sentencing Act 2020 increases the general limit on custodial sentence for summary offences in magistrates' court from six to twelve months.)

Section 188: Sharing or threatening to share intimate photograph or film

789 This section creates three new offences of sharing an intimate photograph or film, and one new offence of threatening to share an intimate photograph or film by means of inserting three new sections into the Sexual Offences Act 2003.

Section 66B: Sharing or threatening to share intimate photograph or film

790 Subsection (1) creates a new offence which is committed if a person (A) intentionally shares a photograph or film which shows, or appears to show, another person (B) in an intimate state, without the consent, or a reasonable belief in the consent of that person. There is no requirement to prove the sharing was done for a particular reason. The focus on photographs and films which "shows or appears to show" ensures that the offence is made out, not just in scenarios where the photograph or film shared is a genuine photograph or film of B, but also, for example, where the photograph or film shows someone who appears to be B but might not, in fact, be B (for example, if the photograph or film depicts either B, or B's identical twin C), and photographs and film that , have been altered or manufactured so that it appears to be a genuine photograph or film of B. This approach is taken in all the offences in this section.

791 Subsection (2) creates a new offence which is committed if a person (A) intentionally shares a photograph or film which shows, or appears to show, another person (B) in an intimate state, without the consent of B, with the intent to cause alarm, distress or humiliation to B.

792 Subsection (3) creates a new offence of intentionally sharing a photograph or film which shows, or appears to show, another person (B) in an intimate state, without the consent or a reasonable belief in the consent of B, for the purpose of obtaining sexual gratification for the person doing the sharing, or another person.

793 Subsection (4) creates a new offence of threatening to share a photograph or film which shows or appears to show another person (B), and where the perpetrator intended that B or someone who knows B will fear the threat will be carried out, or was reckless as to that result.

794 Subsection (5) provides for the offences in subsections (1) – (4) to be subject to section 66C, which sets out a number of exemptions (not all of which would be applicable to all the offences).

795 Subsection (6)(a) provides that, for the purposes of the offences in subsections (1) to (3) and the exemption in 66C(3)(b), "consent" to the sharing of a photograph or film includes consent to share the photograph or film generally, and consent to the particular sharing in question.

796 Subsection 6(b) provides that when determining whether or not a person's belief in B's consent was reasonable, regard must be had to all of the circumstances, including any steps that the person has taken to ascertain whether B consents.

797 Subsections (7)(a) and (b) provides that the threat offence can be made out even if the photograph or film does not exist, or where the photograph or film does exist, it is not in fact a photograph or film which shows or appears to show a person in an intimate state.

798 Subsection (8) provides a defence where the person charged has a reasonable excuse for sharing the photograph or film without consent or a reasonable belief in consent. Examples of a reasonable excuse might include where it was necessary for the prevention or detection of a crime to share an intimate photo or film with a police officer.

799 Subsection (9) provides that the offence in subsection (1) is triable only summarily. The maximum penalty on conviction is imprisonment for a term not exceeding the maximum term for summary offences, which is 6 months if the offence is committed before section 281(5) of the Criminal Justice Act 2003 comes into force, or 51 weeks if committed after that time (subsection 11). An offender may also be given an unlimited fine.

800 Subsection (10) provides for the offences under subsections (2), (3) and (4) to be triable either way (that is, either in a magistrates' court or on indictment by the Crown Court). If convicted in a magistrates' court the maximum penalty on conviction is imprisonment for a term not exceeding the general limit in a magistrates' court (subsection 11). An offender may also be given an unlimited fine. On conviction on indictment the maximum penalty would be imprisonment for a term no more than 2 years.

801 Subsection (12) confers a power on a magistrates' court or jury to find a person guilty of the offence in subsection (1) where they have been found not guilty of one of the more serious offences under subsections (2) or (3), for example because it has not been proven that the person shared the photograph or film for the purpose of obtaining sexual gratification. Where this occurs in the Crown Court, the Court would have the same powers and duties that a magistrates' court would have when convicting a person of a subsection (1) offence (subsection 13) (for example, the maximum penalty will align with that set out in subsection (9)).

Section 66C: Sharing or threatening to share intimate photograph or film: exemptions

802 The exemption in subsection(1) applies where the photograph or film that was shared has been taken in a place to which the public, or a section of the public, had access. This exemption would only apply where the photograph was taken in public; and B was either voluntarily in the intimate state or the defendant reasonably believed they were; and the B did not have a reasonable expectation of privacy against a photograph or film being taken.

803 Subsection (2) provides that whether or not B has a reasonable expectation of privacy from a photograph or film being taken in public is judged by the circumstances that (A) reasonably believes to have existed at the time it was taken. The court would need to determine whether in the circumstances that the defendant reasonably believes them to be, B had a reasonable expectation of privacy from a photograph or film being taken. If the court decides that B would have had a reasonable expectation of privacy from a photograph or film being taken in those circumstances, the exemption is not made out. If the court finds that B would not have had a reasonable expectation of privacy the exemption would apply and the defendant would not have committed the offence.

804 The exemption in subsection (3) provides that where a person shares an intimate photograph or film, and that photograph or film had been previously shared in public, or the person reasonably believed that it had been, and that B had consented to the previous sharing, or the person sharing the photograph had a reasonable belief that they had consented, this is not an offence.

805 The exemption in subsection (4) provides that where a person shares an intimate photograph or film of a child under 16 who lacks capacity to consent to the sharing (or the person sharing reasonably believes they lack capacity to consent), and it is shared for the purpose of the child's care or treatment by a healthcare professional, this is not an offence.

806 The exemption at subsection (5) provides that where a person shares an intimate photograph or film of a child which is of a kind normally shared between family and friends, this is not an offence. It would not be necessary for the intimate photograph or film to have only been shared with family and friends, just that it was that kind of image.

807 By virtue of the exemption at subsection (6) it is not an offence to threaten to share an intimate photograph or film unless the act of sharing the photograph or film in the circumstances conveyed by the threat would be an offence under (66B)(1), (2) or (3).

66D: Sharing or threatening to share intimate photograph or film: interpretation

808 Subsection (1) provides for this section to apply for the purposes of the offences in 66B and the exemptions in 66C.

809 Subsection (2) a person would 'share' something if they, by any means, give or show it to another person, or make it available to another person. This includes electronic sharing, for example by posting a photograph or film on a website or emailing to someone. It also includes the sharing of a physical document, for example by giving a printed photograph to another person or displaying it in a place where other people would see it.

810 Subsection (3) provides that where an internet service provider is the means by which a photograph or film is shared, they would not be regarded as a person who has 'shares' it.

811 Subsection (4) ensures that "photograph" and "film" have the same meaning as section 66A. Subsections (3) and (4) of that provision provides that "photograph" includes the negative as well as the positive version; and "film" means a moving image. Subsection (5) of section 66A provides that "film" and "photograph" would also include images that are made or altered by computer graphics (or in any other way) if they appear to be a photograph or film. It will therefore include genuine photographs or films that have been altered in some way, and those that have been wholly manufactured - so called "deepfake" images. Also included within the definitions of "photograph" and "film" are copies of images which have been made or altered and which appear to be a photograph or film, and data that can be converted into such an image – for instance data stored on a hard drive or disc.

812 Subsection (5) provides that a photograph or film shows or appears to show a person in an "intimate state" if it shows or appears to show them (a) participating or engaging in an act which a reasonable person would consider to be a sexual (for example, engaging in sexual intercourse); (b) doing a thing which a reasonable person would consider to be sexual (for example, posing in a sexually explicit way); (c) all or part of their exposed genitals, buttocks or breasts; (d) in an act of urination or defection, or (3) carrying out an act of personal care associated with their urination, defection or genital or anal discharge. Subsection (5) specifically excludes photographs and film that show, or appear to show, anything that would otherwise meet this definition but that would be ordinarily seen in public (with the exception of breastfeeding) (subsection (8)).

813 Subsection (6) provides that a person's genitals, buttocks or breasts are still considered to be "exposed" under subsection (5)(c), if, although covered by clothing, their genitals, buttocks or breasts are visible through wet or otherwise transparent clothing (subsection (6)(a)). "Exposed" also captures a case where a person's genitals, buttocks or breasts are covered only by underwear (subsection (6)(b)). It would also capture the case where those parts of the anatomy would be exposed but for the fact that they are obscured by something (other than clothing that the person is wearing) which provides a similar or smaller degree of coverage than underwear (subsection (6)(c)). Subsection (7) explains that the relevant part of anatomy can be "obscured" by any means (other than clothing that the person is wearing) including by part of their body, or by digital alteration (for example, if the photograph included an 'emoji' on the person's breasts).

Repeals and amendments in connection with offences

Section 189: Repeals in connection with offences under sections 179 and 181

814 Subsection (1) sets out that subsection (2)(a) and (b) of the section 127 of the Communications Act (false messages) 2003 are repealed in so far as they extend to England, Wales and Northern Ireland. Subsection (2) also repeals section 1(1)(a)(ii), section 1(1)(a)(iii) and section 1(2) of the Malicious Communications Act 1988.

815 Subsection (3) sets out that Article 3(1)(a)(ii), 3(1)(a)(iii) and 3(2) of the Malicious Communications (Northern Ireland) Order 1988 (S.I. 1988/1849 (N.I. 18)) are repealed.

Section 190: Repeals in connection with offences under section 188

816 This section sets out that sections 33 to 35 of the Criminal Justice and Courts Act 2015 are repealed.

Section 191: Consequential amendments

817 This section sets out in which part of Schedule 14 the consequential amendments in connection with the offences created in sections 179, 181, 183, 184, 187, 188 and 190 can be found.

Schedule 14: Amendments consequential on offences in Part 10 of this Act

Part 1

Amendments consequential on offences in sections 179, 181 and 183

Football Spectators Act 1989

818 Paragraph 1 of Schedule 14 amends Schedule 1 of the Football Spectators Act 1989 (football banning orders: relevant offences) to reflect references to the new false and threatening communications offences under the Online Safety Act 2023.

Sexual Offences Act 2003

819 Schedule 5 of the Sexual Offences Act 2003, in the list of offences for England and Wales, lists offences in connection with which a sexual harm prevention order may be made. Paragraph 2 of Schedule 14 adds to this list an offence under section 179 of the Online Safety Act 2023 (false communications); and an offence under section 181 of that Act (threatening communications).

820 Paragraph 3 updates Schedule 5 of the Sexual Offences Act 2003, in the list of offences for Northern Ireland, to include references to sections 180 and 182 (false and threatening communications offences).

Regulatory Enforcement and Sanctions Act 2008

821 Paragraph 4 updates Schedule 3 of the Regulatory Enforcement and Sanctions Act 2008, to include references to section 179 and 181 (false communications and threatening communications offences).

Elections Act 2022

822 Paragraph 5 refers to the offences in Schedule 9 of the Elections Act 2022 (disqualification from holding elective office) and inserts references to section 179, 181 and 183 (false communications, threatening communications and sending or showing flashing images).

Offence to be inserted into Sexual Offences Act 2003

Section 187: Sending etc photograph or film of genitals

823 This section creates a new offence of sending etc a photograph or film of a person's genitals to another person, in England and Wales. It inserts a new section 66A into the Sexual Offences Act 2003 ("the 2003 Act"). Section 66A(1) provides that where a person (A) intentionally sends or gives a photograph or film of any person's genitals to another person (B), and either A intends that B will see the genitals and be caused alarm, distress or humiliation, or A sends or gives the photograph or film for the purpose of obtaining sexual gratification and is reckless as to whether B will be caused alarm, distress or humiliation, A commits an offence.

824 Subsection (2) makes clear that "sending or giving" a photograph or film includes, in particular, sending it to another person by any means, electronically or otherwise, showing it to another person, and placing it for a particular person to find.

825 Subsections (3) to (5) set out what is meant by "photograph" and "film". In particular, subsection (5) makes clear that references to the terms include an image, whether made by computer graphics or in any other way, which appears to be a photograph or film; a copy of such an image, photograph, or film, and data stored by any means which is capable of conversion into such an image; photograph, or film.

826 Subsection (6) provides that the offence is triable either way. Following summary conviction, the maximum penalty is six month's imprisonment prior to the coming into force of paragraph 24(A) of Schedule 22 to the Sentencing Act 2020 upon and twelve months' thereafter. (Paragraph 24(A) of Schedule 22 to the Sentencing Act 2020 increases the general limit on custodial sentence for summary offences in magistrates' court from six to twelve months.)

Part 2

Amendments consequential on offence in section 184

Children and Young Persons Act 1933

827 Paragraph 6 amends Schedule 1 to the Children and Young Person Act 1933 (offences against children and young persons with respect to which special provisions of Act apply) to include an offence under section 184 where the relevant act is an act capable of, and done with the intention of, encouraging or assisting the serious self-harm of a child or young person.

Visiting Forces Act 1952

828 Paragraph 7 amends the Schedule to the Visiting Forces Act 1952 to include an offence under section 184.

Children and Young Persons Act (Northern Ireland) 1968 (c. 34 (N.I.))

829 Paragraph 8 amends Schedule 1 to the Children and Young Persons (Northern Ireland) Act 1968 in the same way that paragraph 6 amends Schedule 1 to the Children and Young Persons Act 1933.

Criminal Attempts Act 1981

830 Paragraph 9 amends section 1 of the Criminal Attempts Act 1981 to ensure that the offence of attempting to commit an offence, contrary to that Act, does not apply to an offence under section 184 because the offence of encouraging or assisting serious self-harm is itself an inchoate offence.

Criminal Attempts and Conspiracy (Northern Ireland) Order 1983 (S.I. 1983/1120 (N.I. 13))

831 Paragraph 10 amends Article 3 of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983 in the same way that paragraph 9 amends section 1 of the Criminal Attempts Act 1981.

Armed Forces Act 2006

832 Paragraph 11 amends Schedule 2 to the Armed Forces Act 2006 to include an offence under section 184.

Serious Crime Act 2007

833 Paragraph 12 amends section 51A of and Part 2 of Schedule 3 to the Serious Crime Act 2007 to ensure that the offence of encouraging or assisting an offence contrary to section 44 of that Act does not apply to an offence under section 184 because the offence of encouraging or assisting serious self-harm is itself an inchoate offence.

Part 3

Amendments consequential on offences in sections 187 and 188

Children and Young Persons Act 1933

834 Paragraph 13 amends Schedule 1 of the Children and Young Persons Act 1933 (offences against children and young persons with respect to which special provisions of Act apply) to refer to section 66A and 66B in the entry relating to the Sexual Offences Act 2003.

Police and Criminal Evidence Act 1984

835 Paragraph 14 adds a reference to the new offence of sending etc photograph or film of genitals, and certain of the new offences of sharing or threatening to share an intimate photograph or film to section 65A(2) of the Police and Criminal Evidence Act 1984 meaning of "qualifying offence" for the purposes of Part 5 of that Act.

Sexual Offences (Amendment) Act 1992

836 Paragraph 15 applies the provisions of the Sexual Offences (Amendment) Act 1992 to the person shown, or who appears to be shown in an intimate photograph or film where a threat to share the photograph or film was made to someone else.

Sexual Offences Act 2003

837 Paragraph 16 amends the Sexual Offences Act 2003.

838 Subparagraph (2) provides that the definition of "sexual" in section 78 of the Sexual Offences Act 2003 does not apply to the new offences of sharing and threatening to share an intimate photograph or film on account of a separate definition applying to those offences.

839 Subparagraph (3) adds a reference to the new offence of sending etc photograph or film of genitals (section 66A) and certain of the new offences of sharing an intimate photograph or film (section 66B(2)) and (3) to section 136A(3A) of the Sexual Offences Act 2003 (offences specified as child sex offences for the purposes of Part 2A of that Act when committed against a person under 18).

840 Sub-paragraph (4) adds a reference to the new offence of sending etc photograph or film of genitals (section 66A) and the new offence of sharing an intimate photograph or film for the purpose of obtaining sexual gratification (section 66B(3))to Schedule 3 to the Sexual Offences Act 2003 (offences to which certain provisions of that Act apply).

Criminal Justice Act 2003

841 Paragraph 17 amends the Criminal Justice Act 2003.

842 Sub-paragraph (2) adds a reference to the new offence of sending etc photograph or film of genitals (section 66A), and certain of the new offences of sharing an intimate photograph or film, sections 66B(2) and 66B(3) to Part 2 of Schedule 15 (specified sexual offences for purposes of section 325) and sub-paragraph (3) adds a reference to the new offence of sending etc photograph or film of genitals (section 66A) and certain of the new offences of sharing an intimate photograph or film, (sections 66B(2)) and 66B(3) to Schedule 34A (child sex offences for purposes of section 327A).

Anti-social Behaviour, Crime and Policing Act 2014

843 Paragraph 18 adds a reference to sections 66A, 66B(2) and 66B(3) to section 116 of the Anti-social Behaviour, Crime and Policing Act 2014 (conduct constituting offence amounting to "child exploitation" when committed against a person under 18 for the purposes of that section).

Modern Slavery Act 2015

844 Paragraph 19 adds a reference to sections 66A, 66B(2) and 66B(3) to paragraph 33 of Schedule 4 to the Modern Slavery Act 2015 (offences to which the defence in section 45 does not apply).

Sentencing Act 2020

845 Paragraph 20 amends Part 2 of Schedule 18 to the Sentencing Act 2020 (specified sexual offences for the purposes of section 306) to refer to section 66A, section 66B(2) and section 66B(3) under paragraph 38 (offences under Sexual Offences Act 2003).

Elections Act 2022

846 Paragraph 21 amends Schedule 9 of the Elections Act 2022 (offences for the purposes of Part 5) to refer to section 66A (sending etc of photograph or film of genitals).

Part 4

Amendments consequential on section 190

Criminal Justice and Courts Act 2015

847 Paragraph 22 amends section 96 of the Criminal Justice and Courts Act 2015 to remove reference to the offence at section 33 of that Act ("Disclosing or threatening to disclose private, sexual photographs or films with intent to cause distress") which is repealed by section 190 of this Act. Paragraph 22 also removes Schedule 8 to the Criminal Justice and Courts Act 2015 which makes provisions for section 33 of that Act.

Domestic Abuse Act 2021

848 Paragraph 23 removes section 69 of the Domestic Abuse Act 2021 which amends section 33 of the Criminal Justice and Courts Act 2015 ("Disclosing or threatening to disclose private sexual photographs or films with intent to cause distress") which is repealed by section 190 of this Act. Paragraph 23 also amends sections 85 and 91 of the Domestic Abuse Act 2021, to remove references to section 69 of that Act.

Overseas Operations (Service Personnel and Veterans) Act 2021

849 Paragraph 24 amends Part 1 of Schedule 1 to the Overseas Operations (Service Personnel and Veterans) Act 2021 to remove reference to the offence at section 33 of the Criminal Justice and Courts Act 2015 ("Disclosing or threatening to disclose private sexual photographs or films with intent to cause distress") which is repealed by section 190 of this Act.

Criminal Justice (Electronic Commerce) (Amendment) (EU Exit) Regulations 2021 (S.I. 2021/835)

850 Paragraph 25 amends the Criminal Justice (Electronic Commerce) (Amendment) (EU Exit) Regulations 2021 to remove reference to the offence at section 33 of the Criminal Justice and Courts Act 2015 ("Disclosing or threatening to disclose private, sexual photographs or films with intent to cause distress") which is repealed by section 190 of this Act.

Part 11: Supplementary and General

Providers' judgements about the status of content

Section 192: Providers' judgements about the status of content

851 This section clarifies how providers of Part 3 services are to approach judgements (human or automated) about whether content is content of a particular kind (such as illegal content, content that is harmful to children, etc), when their risk assessments or systems and processes for compliance with the Act involve such judgments. In particular, it makes provisions about how questions of mental state and defences are to be approached when considering whether content is illegal content or a fraudulent advertisement.

852 Subsection (2) requires that such judgments must be made on the basis of all the relevant information that is reasonably available to a provider.

853 Subsection (3) specifies factors that are particularly relevant to the question of what information is "reasonably available" to a provider. It makes clear that the requirement in subsection (2) applies both to judgements made by human moderators and those made by automated systems and processes, but that the information reasonably available to an automated system or process might be construed to be different to the information reasonably available to human moderators.

854 Subsections (5), (6) and (7) apply specifically to judgements about whether content is illegal content or a fraudulent advertisement.

855 Subsection (5) and (6) require providers to treat content as illegal content or a fraudulent advertisement if, on the basis of all information reasonably available to the provider, there are reasonable grounds to infer all the elements - including mental elements such as intention - necessary for the commission of a relevant offence are present, and there are not reasonable grounds to infer a defence may be relied upon.

856 Subsection (7) makes provision for judgements about whether content that is generated by bots is illegal content or a fraudulent advertisement, including in particular how providers should consider mental elements and defences relating to content generated by bots. Section 55(4) of

the Act makes clear that content generated by bots can, in certain circumstances, be 'user-generated content' for the purposes of the Act, and so can be in-scope of Part 3 services' duties.

857 Subsection (8) clarifies that when OFCOM consider a provider's compliance with making content judgements, it may take into account whether providers' judgements follow the approaches set out in this section (including judgements made by means of automated systems or processes, alone or together with human moderators).

Section 193: OFCOM's guidance about illegal content judgements

858 Subsection (1) and (2) require OFCOM to produce guidance for providers of Part 3 services about how they should approach judgements about whether content is illegal content or a fraudulent advertisement, and whether news publisher content amounts to a relevant offence.

859 Subsections (3) and (4) require that OFCOM must consult appropriate persons before creating the guidance, and must publish the guidance.

Time-limits for first guidance

Section 194: Time for publishing first guidance under certain provisions of this Act

860 Subsection (1) sets out that OFCOM must publish certain guidance documents within 18 months of the day the Act is passed. Subsection (2) sets out which guidance documents this applies to.

861 Subsection (3) allows OFCOM to extend the 18 month period by up to 12 months by making and publishing a statement. Subsection (4) sets out that OFCOM's statement must give their reasons for doing this and the period of the extension.

862 Subsection (5) allows OFCOM to publish this statement at the same time as, or incorporate, a statement under section 43(12), which contains similar provision about extending the time period for issuing certain draft codes of practice.

863 Subsection (6) sets out that a statement cannot be made in relation to guidance mentioned in a particular paragraph of subsection (2) if a statement has previously been made under subsection (3) or section 43(12). In effect, OFCOM may only extend the 18 month period a single time.

Liability of providers etc

Section 195: Providers that are not legal persons

864 This section provides for the situation in which a penalty notice or confirmation decision needs to be given to a provider of a regulated service that is not a legal person. This may occur, for example, where a partnership or an unincorporated association (an organisation set up through an agreement between a group of people who come together for a reason other than to make a profit, such as a voluntary group or a sports club) provides a regulated service.

Section 196: Individuals providing regulated services: liability

865 This section sets out how various provisions of the Act may apply to a group of two or more individuals who together are providers of a regulated service. Where two or more individuals together are providers of a regulated service, they will be jointly and severally liable for any duty, requirement or liability to pay a fee. Two or more individuals jointly given a penalty notice or confirmation decision will also be jointly and severally liable to pay the penalty or meet the requirements.

866 The section also provides for how penalty notices or confirmation decisions may be given to individuals who are together providers.

Section 197: Liability of parent entities etc

867 This section cross-refers to Schedule 15, which contains provisions about how joint liability operates under the Act.

Schedule 15: Liability of parent entities etc

Joint provisional notices of contravention

868 Schedule 15 establishes that decisions or notices can be given jointly to both a regulated provider and its parent company (or controlling individual(s)), its subsidiary company or a fellow subsidiary.

869 All relevant entities must be given the opportunity to make representations when OFCOM are seeking to establish joint liability, including on the matters contained in the decision or notice and whether joint liability would be appropriate.

870 When OFCOM issue decisions or notices to multiple parties, they are all jointly liable to comply with any requirements or penalties imposed.

Section 198: Former providers of regulated services

871 This section makes clear that OFCOM's powers to issue enforcement notices, including notices relating to the duty to cooperate with an investigation, may be given to a former provider of a regulated service. OFCOM can issue an enforcement notice to a former service provider if, at the relevant time, the provider was operating a regulated service.

Offences

Section 199: Information offences: supplementary

872 This section sets out further detail on how the information offences in section 109(1) and paragraph 18(1)(b) of Schedule 12 operate.

873 Proceedings against a person for an offence of failing to comply with requirements in an information notice or failing to comply with any requirement imposed by a person authorised by OFCOM to exercise powers of entry and inspection may be brought only if:

a. The person has been given a provisional notice of contravention;

b. They have received a confirmation decision in respect of that failure (requiring them to comply with the original requirement or remedy their failure to comply with it) and they have not complied with its requirements by the deadline it sets;

c. A penalty has not been imposed on them by OFCOM in respect of that failure; and

d. Neither a service restriction order nor an access restriction order has been made in relation to a regulated service provided by them in respect of that failure.

874 Subsection (2) confirms that, if any proceedings are to be brought against a senior manager for the offence of failing to prevent an offence of failing to comply with an information notice, these conditions must also be met in relation to the failure to comply with an information notice.

Section 200: Offence of failure to comply with confirmation decision: supplementary

875 This section ensures that, among other things, a person cannot be prosecuted for the new confirmation decision offences where OFCOM has imposed a financial penalty for the same conduct instead, and vice versa.

Section 201: Defences

876 This section applies where a person relies on a defence under section 109 or 110.

877 Where a defendant adduces evidence which raises an issue with respect to the defence, the burden is on the prosecution to prove beyond reasonable doubt that the defence is not satisfied.

Section 202: Liability of corporate officers for offences

878 This section means that in certain circumstances 'corporate officers' of regulated providers may be found liable for information offences committed by that entity. Corporate officers are generally directors, managers or similarly senior employees.

879 If an offence is found to be committed by an entity, and that offence is proved to have been committed with the consent, connivance or neglect of a corporate officer, both the officer and the relevant entity can be found guilty of the offence.

Section 203: Application of offences to providers that are not legal persons

880 This section sets how information offences apply to providers that are not legal persons under the law under which they are formed. Under English and Welsh law, a partnership and an unincorporated association would both be examples of such entities.

881 Subsection (2) specifies that proceedings for an offence under this Act alleged to have been committed by a relevant entity must be brought against the entity in its own name. It must not be brought in the name of any of its officers, members or partners. For such proceedings, the rules of court relating to service of documents have the same effect as if the entity were a body corporate (e.g. a company), and that the listed provisions in subsection (3)(b) also apply as they would apply in relation to a body corporate. A fine imposed on a relevant entity on its conviction of an offence under this Act is to be paid out of the entity's funds.

882 Subsection (5) provides that, if the relevant entity commits an offence, and this offence was committed with the consent or connivance of, or can be attributed to the neglect of, an officer, then the officer also commits the offence. Proceedings may thus be brought against the officer (subject to section 199(1)) and they may be punished accordingly. The liability of an officer under this subsection is not prejudiced by subsection (2).

Extra-territorial application

Section 204: Extra-territorial application

883 This section specifies that references to internet services, user-to-user services and search services and OFCOM's information-gathering powers apply to services provided from outside the United Kingdom (as well as to services provided from within the United Kingdom).

Section 205: Offences: extra-territorial application and jurisdiction

884 This section outlines that the information offences in the Act apply to acts done in the United Kingdom and outside of the United Kingdom. All offences can be prosecuted in any part of the United Kingdom as if they occurred in that part of the United Kingdom.

Payment of sums into the Consolidated Fund

Section 206: Payment of sums into the Consolidated Fund

885 This section amends section 400 of the Communications Act 2003 so that it applies to amounts paid to OFCOM in respect of penalties imposed under the Online Safety Act 2023, and in respect of fees charged under Schedule 10. This section requires OFCOM to pay any penalty sums, and any fees under Schedule 10, they receive into the Consolidated Fund of the United Kingdom.

Publication by OFCOM

Section 207: Publication by OFCOM

886 This section requires OFCOM to publish anything they must publish under the Act in a way which is appropriate to bring it to the attention of any audience likely to be affected by it.

Service of notices

Section 208: Service of notices

887 This section sets out the process for serving any notices or decisions under the Act, including notices to deal with CSEA or terrorism content, information notices, enforcement notices, penalty notices and public statement notices to providers of regulated services both within and outside of the United Kingdom.

Repeals and amendments

Section 209: Amendments of Part 4B of the Communications Act

888 This section introduces a new Schedule (Amendments of Part 4B of the Communications Act) to amend the Video-Sharing Platform (VSP) regime contained in Part 4B of the Communications Act to ensure the regime remains effective until it is repealed.

Schedule 16: Amendments of Part 4B of the Communications Act

889 This Schedule makes amendments to Part 4B of the Communications Act, which regulates Video-Sharing Platform (VSP) services, to address changes required to the United Kingdom's VSP regime as a result of the United Kingdom's exit from the EU and to ensure the regime remains effective until it is repealed. Amendments include removing references to EU law, and allowing OFCOM to cooperate with EEA states.

Section 210: Repeal of Part 4B of the Communications Act

890 This deletes sections pertaining to the regulation of Video-Sharing Platform services from the Communications Act 2003, the Audiovisual Media Services Regulations 2020 and the Audiovisual Media Services (Amendment) (EU Exit) Regulations 2020.

Section 211: Repeal of Part 4B of the Communications Act: transitional provision etc

891 This section introduces Schedule 17 (Video-Sharing Platform services: transitional provision etc) which contains transitional, transitory and savings provisions relating to the repeal of the Part 4B of the Communications Act 2003, which contains the regulatory regime for the regulation of Video-Sharing Platform services. This section also gives the Secretary of State a power to make regulations containing further transitional, transitory or savings provisions.

Schedule 17: Video sharing platform services: transitional provision etc

892 This Schedule contains transitional, transitory and saving provisions setting out how the Video-Sharing Platform (VSP) regime in Part 4B of the Communications Act 2003 will be repealed and how the Online Safety Act 2023 will apply during the "transitional period".

893 Part 2 of Schedule 17 sets out that the Online Safety Act 2023 applies to VSPs (that meet the definition set out in Schedule 17, paragraph 1); however, for the duration of the transitional period, they will be exempted from certain Online Safety Act 2023 duties and requirements. During this transitional period, these VSPs will continue to be regulated under the VSP regime. Broadly, where an internet service is wholly a VSP (Schedule 17, paragraph 1(1)(a)), the exemption applies to the service as a whole. However, where only a "dissociable section" of an internet service is a VSP (Schedule 17, paragraph 1(1)(b)), the exemption will only apply to the VSP part. However, VSPs will still be subject to the new communications offences, OFCOM's information powers and associated enforcement powers, and fee notification requirements. VSPs will also become subject to the requirement to complete children's access and risk assessments once a date is specified by the Secretary of State via regulations.

894 Part 3 of Schedule 17 sets out the application of Part 6 of the Online Safety Act 2023 in respect of transitional charging years. The transitional arrangements require that VSPs provide notification of eligibility to pay fees and provide financial information to OFCOM under section 83.

895 Where a VSP is an "exempt provider", the provider does not have to pay fees under section 84 or Schedule 10, during a transitional charging year. Where a VSP is not an "exempt provider" (i.e. it is an internet service with a "dissociable section" that is a VSP, and it has either another user-to-user part or search engine part that is not a VSP), if Schedule 17 paragraph 17(2) applies, their fee notification must include a breakdown indicating the amounts that are wholly referable to the VSP part. If a VSP is not an exempt provider, they are subject to the duty to pay fees under section 84 or Schedule 10 in respect to a transitional charging year.

896 In calculating providers fees, the qualifying worldwide revenue (QWR) is to be taken as the "non-Part 4B QWR" i.e. the QWR less the amounts wholly referable to the VSP part. As per section 84(3), in the event of a disagreement between the provider and OFCOM regarding the "non-Part 4B QWR" or fees payable, the amount is determined by OFCOM.

897 The transitional arrangements for VSPs will end on the date on which section 210 of the Act, which repeals Part 4B of the Communications Act 2003, comes into force (with the exception of Schedule 17, Part 3, which applies in respect to a transitional charging year). Section 210(3) ensures that Part 4B may not be repealed until at least 6 months after the chosen date for the obligation to conduct risk and child access assessments (to give providers time to do their assessments before they become subject to the safety duties).

898 The savings provisions in Schedule 17, Part 4 allow OFCOM to continue to pursue ongoing enforcement action, relating to breaches of Part 4B of the Communications Act 2003 that occurred while it was in force, after the repeal of that Part.

Section 212: Repeals: Digital Economy Act 2017

899 This section repeals Part 3 of the Digital Economy Act 2017 (which makes provision in relation to online pornography and an age verification system) and removes the obligation for the Secretary of State to issue a code of practice for online service providers by repealing section 103 of that Act. As a consequence of the repeal of Part 3, the power to extend it to the Channel Islands or the Isle of Man is also repealed.

Section 213: Offence under the Obscene Publications Act 1959: OFCOM defence

900 This section amends section 2 of the Obscene Publications Act 1959, to create a defence for employees of OFCOM and those assisting OFCOM in the exercise of OFCOM's online safety functions regulatory functions under the Online Safety Act 2023.

901 It inserts an additional subsection into the 1959 Act to create a defence for the offence of publishing an obscene article the effect of which is to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it. This applies where the defendant is a member of OFCOM, employed or engaged by OFCOM or assisting OFCOM in the exercise of their online safety functions and the publication of the obscene article is made for the purpose of any of OFCOM's online safety functions, as defined in section 235.

902 We expect that the handling of this material may be necessary in the course of OFCOM's delivery of their online safety functions, as services will be required by duties in the legislation to proactively identify and remove this content. For example, OFCOM may be required to handle this material when assessing a services' systems and processes to assess how they handle illegal content.

Section 214: Offences regarding indecent photographs of children: OFCOM defence

903 This section amends section 1B of the Protection of Children Act 1978 (defence to offence relating to indecent photographs of children) to create a defence for OFCOM when exercising their online safety functions.

904 It inserts an additional section into the 1978 Act to create a defence for the offence of making an indecent photograph or pseudo-photograph of a child in circumstances where the defendant is a member of OFCOM, employed or engaged by OFCOM or assisting OFCOM in the exercise of their online safety functions and the photograph or pseudo-photograph is made for the purpose of any of OFCOM's online safety functions, as defined in section 206 of the 1978 Act. It is expected that the handling of this material may be necessary in the course of OFCOM's delivery of their online safety functions, as services e are required by duties in the legislation to proactively identify and remove this content. An example of a scenario in which OFCOM may be required to handle this material would be if OFCOM is assessing a services' systems and processes to assess how they handle illegal content or needs to show that a service is not handling complaints about illegal content correctly.

905 The section provides for amendment to the equivalent legislation in Scotland (Section 52 of the Civic Government (Scotland) Act 1982 (indecent photographs of children)) and in Northern Ireland (Article 3A of the Protection of Children (Northern Ireland) Order 1978 (defence to offence relating to indecent photographs of children)).

Powers to amend Act to regulate app stores

Section 215: Powers to regulate app stores

906 This section allows the Secretary of State to make regulations to amend the Act to bring app stores within its scope. The regulations may not be made until OFCOM has published its report about the use of app stores by children. The Secretary of State may make regulations imposing requirements on app stores if, having considered OFCOM's report, they consider that there is a material risk of significant harm to children either on or by means of the app store (i.e. through the apps a child accesses).

Section 216: Powers to regulate app stores: supplementary

907 This section makes provisions about the purpose and contents of regulations to regulate app stores under section 215.

Powers to amend Act: alternative dispute resolution

Section 217: Powers to impose duty about alternative dispute resolution procedure

908 This section provides the Secretary of State with the power to make regulations to place a requirement on providers of Category 1 services to arrange for, and engage in, an out of court, impartial alternative dispute resolution procedure (ADR duty).

909 The Secretary of State has the power to make regulations to amend the Act in connection with the imposition on providers of Category 1 services of an ADR duty, with a non-exhaustive list of specific sections which may be amended set out at subsections (7) and (8). Regulations under this section cannot be made before the publication of a statement by the Secretary of State responding to OFCOM's report about the content reporting and complaints procedures operated by providers of Part 3 services (see section 160).

910 If the Secretary of State does exercise the power to make regulations making providers of Category 1 services subject to an ADR duty, the regulations also need to include provisions requiring OFCOM to (following consultation) produce guidance for providers of Category 1 services to assist their compliance with that duty.

Other powers to amend Act

Section 218: Power to amend section 40

911 This section gives the Secretary of State the power to amend the list of fraudulent offences in section 40 in relation to the duties about fraudulent advertising. This power is subject to some constraints.

912 Subsection (2) lists the criteria any further offence must meet before the Secretary of State may include it in the list of fraudulent offences in section 40. Subsection (3) further limits the Secretary of State's power to include new fraud offences, listing types of offences which may not be added to section 40. This is to avoid regulatory duplication.

Section 219: Powers to amend sections 61 and 62

913 This section relates to section 61 and 62 which describe the categories of primary priority and priority content that is harmful to children.

914 Subsection (1) confers a power on the Secretary of State to make regulations to amend these sections, i.e. to amend the categories of primary priority and priority content that is harmful to children.

915 Subsections (2) and (3) constrain this power. The Secretary of State can only add a kind of content to the categories of primary priority or priority content under this power if they consider that there is a material risk of significant harm to an appreciable number of children in the United Kingdom presented by regulated user-generated or search content of that kind. Under subsection (2)(b), to add a kind of content as primary priority content that is harmful to children, the Secretary of State must also consider it appropriate for the duties in sections 12(3)(a) and 29(3)(a) to apply to it (i.e. to require user-to-user services to use systems and processes designed to prevent children of all ages from encountering that kind of content, and to require search services to use systems and processes designed to minimise the risk of children of all ages from encountering that kind of content).

916 Subsection (4) further limits the kinds of content that can be added to section 61 or 62 as primary priority or content that is harmful to children, by reference to the way in which content presents a risk of harm.

917 The Secretary of State is required by subsection (5) to consult OFCOM before making regulations under this power.

Section 220: Powers to amend or repeal provisions relating to exempt content or services

918 This section allows the Secretary of State to make regulations to amend or repeal provisions relating to exempt content or services if the Secretary of State considers that it is appropriate to do so because of the risk of harm to individuals in the United Kingdom presented by the relevant content or services. Regulations made under this section can be used to exempt certain content or services from the scope of the regulatory regime or to bring them into scope.

919 Subsection (3) provides that these powers cannot be used to bring comments on news publisher sites within the definition of "regulated user-generated content" in Part 3 (see section 55).

Section 221: Powers to amend Part 2 of Schedule 1

920 Paragraph 10 of Schedule 1 exempts user-to-user or search services that are provided by education or childcare providers described in Part 2 of Schedule 1 from relevant duties under the Act where those services are provided for the purpose of education and childcare. This section provides a set of powers to amend the list of exempt education and childcare providers listed in Part 2 of Schedule 1. This includes powers for the Secretary of State to amend the list in Part 2 of Schedule 1 which relates to England and for the relevant Devolved Ministers to amend the lists for their respective areas. This section also sets out the criteria that must be met in order for amendments to be made.

Section 222: Powers to amend Schedules 5, 6 and 7

921 This section gives the Secretary of State power to amend the three Schedules which list the criminal offences that are priority offences, as defined in section 59(7).

922 The Secretary of State may amend the list of terrorism offences and the list of CSEA offences other than those CSEA offences which extend only to Scotland, which may be amended by the Scottish Ministers. The Secretary of State may also amend Schedule 7 (priority offences), but the Secretary of State may only add an offence to Schedule 7 if the Secretary of State considers it appropriate for the reasons set out in subsection (4) and if the amendment would not add an offence of a type listed in subsection (6). The Secretary of State must consult with Scottish Ministers before making changes to offences in Schedule 7 that only extend to Scotland, and with the Department of Justice in Northern Ireland before making changes to offences that only extend to Northern Ireland.

Regulations

Section 223: Power to make consequential provision

923 This section gives the Secretary of State a power to make consequential provisions relating to this Act or to regulations under this Act. The power is exercised by regulations and includes the power to amend the Communications Act 2003.

924 This power cannot be exercised so as to include comments and reviews on content on services provided by recognised news publishers within the definition of "regulated user-generated content", and the power to amend Paragraph 4 of Schedule 1 (limited functionality services) cannot be exercised so as to remove such services which are provided by recognised news publishers from that exemption.

Section 224: Regulations: general

925 This section sets out how the powers to make regulations conferred on the Secretary of State can be used. Regulations made under this Act can make different provisions for different purposes, in particular relating to different types of services.

Section 225: Parliamentary procedure for regulations

926 This section sets out the Parliamentary procedure that must be followed when regulations made using powers conferred by the Act are made.

Part 12: Interpretation and final provisions

Interpretation

Section 226: "Provider" of internet service

927 This section determines who is the 'provider' of an internet service, and therefore who is subject to the duties imposed on providers. For user-to-user services, subsections (2) and (3) set out that the provider is the entity (or individual(s)) that controls who can use the user-to-user elements of a service. The duties therefore apply to the entity or person that directly controls users' access to the functionality that enables users to interact or share user-generated content, rather than on any other entity that may embed that service or control other aspects of it. This also makes clear to which entity within a broader corporate structure the duties apply.

928 Subsections (4) and (5) set out that a provider of a search service is the entity (or individual(s)) that has direct control over the operations of the search engine. As set out in subsection (13), the operations of the search service are taken to mean operations which enable users to make search requests, and which subsequently generate responses to those requests. The duties therefore apply to the person or entity that controls which search results appear to users and how they appear, rather than on any other entity that may embed or otherwise use a search engine.

929 Subsections (6) and (7) provide that the provider of a combined service is the entity which meets both definitions in the preceding four subsections. If the entity (or individual(s)) which controls who can use the user-to-user part of the service is different from the entity (or individual(s)) which controls the search engine, it will not be a combined service (see the definition of "combined service" in section 4(7)).

930 Subsections (8) and (9) provide that the provider of an internet service which is neither a user-to-user service nor a search service is the entity (or individual(s)) which has control over which content is published or displayed on the service. This is relevant for determining which entities have duties under Part 5.

931 Subsections (10) and (11) clarifies who counts as the provider of a service (other than a user-to-user or search service) hosting pornographic content for the purposes of the Act. These subsections make clear that a person who controls a tool which generates content on the service which they provide, such as a generative artificial intelligence bot, is to be regarded as controlling the content generated by that tool.

932 Subsection (12) clarifies that someone who provides an access facility in relation to a user-to-user service, which is a facility that can be withdrawn, adapted or manipulated in order to impede access to the user-to-user service (see section 146(10)), is not a provider of that service. This therefore excludes companies which provide infrastructure to other services on a business-to-business basis.

933 Examples of "access facilities" include internet access services, web hosting services, domain name services, software as a service products, security software, content delivery network services, app stores, payment service providers and enterprise software.

Section 227: "User", "United Kingdom user" and "interested person"

934 This section defines the terms "user", "United Kingdom user", and "interested person" in relation to regulated services.

935 Subsection (1) makes clear that a "United Kingdom user" can be either an individual who is in the United Kingdom, or an entity which is incorporated or formed under the law in any part of the United Kingdom.

936 Subsections (3) and (4) outline the circumstances where someone would not be counted as a "user" of a service because they are using the service in the course of the service provider's business. For example, the intention is that an employee of a social media company would not count as a user if uploading content to the service in the course of their employment, for example a company blog. However, they would count as a user of the service if uploading content to that service in a personal capacity.

937 Subsection (7) defines an "interested person" in relation to search services and combined services. This is intended to recognise that these services' actions may affect people and entities who do not directly use search engines where search engines index their website or database.

Section 228: "Internet service"

938 This section sets out the meaning of the term "internet service", which includes services made available by the internet, or by a combination of the internet and an electronic communications service (as defined in section 32(2) of the Communications Act 2003). For example, a service which is partly made available over the internet and partly by routing through the public switched telephone network would count as an internet service. This definition captures services accessed by a mobile phone application as well as those accessed via an internet web browser.

Section 229: "Search engine"

939 This section sets out the meaning of "search engine". This is relevant to the definition of "search service" in section 3(4), which is an internet service that is, or includes, a search engine.

940 Subsection (1)(a) defines a search engine as including services or functionalities which allow a user to search some websites or databases, as well as services which allow a user to hypothetically search *all* websites or databases. This differentiation ensures that search engines and vertical search engines are both included. A vertical search engine is a search engine that is only focused on a specific topic or a genre of content, such as a search engine that only indexes academic articles. Subsection (1)(b) clarifies that the definition does not include services where a user can only search one website or database, thereby ensuring that websites which only have a search tool internal to the website are not considered search services.

941 Subsection (2) makes clear that for a service to be a combined service it is necessary for the entity which would be defined as the provider in relation to the user-to-user part of the service to be the same as the entity which would be defined as the provider in relation to the search engine (although a single entity may be the provider of more than one service).

Section 230: "Age verification" and "age estimation"

942 This section defines age verification and age estimation, and makes it clear that self-declaration of age, unless combined with other measures, does not count as either.

943 In all instances where age verification or age estimation is mandated or permitted for compliance with duties under the Act, there is no requirement in the Act for the age verification or age estimation to be carried out directly by the regulated service provider itself. A regulated service provider may instead use a third party age verification or age estimation service.

944 Age verification means any measure designed to verify the exact age of users of a regulated service. Where a regulated service provider relies on third party age verification for compliance with an obligation under the Act, the result passed to the regulated service provider may be the user's exact age, confirmation that the user is above or below a specified age, or confirmation that the user is within a specified age range, provided that this result has been obtained through age verification.

945 Age verification and age estimation must be used to comply with the new duties introduced for section 12, which requires service providers to use proportionate systems and processes designed to prevent children of any age from accessing primary priority content (as set out in section 61) on their service, and for section 82 which requires providers of services to use age verification or age estimation (or both) to prevent children from encountering regulated provider pornographic content.

946 Age verification and age estimation may also be used to comply with duties under section 12(2) or (3) in circumstances where no specific duty to use age verification or age estimation applies (see section 12(7)) and may also be used to comply with duties under section 29(2) or (3).

947 Age verification or age estimation must also be used if a provider seeks to conclude that children cannot access a service or part of a service, meaning that particular duties under Part 3 of the Act would not apply (see sections 12 and 29 in relation to safety duties protecting children, section 20(4) in relation to content reporting, section 21(5)(a) in relation to complaints procedures, and section 35(2) in relation to children's access assessments).

Section 231: "Proactive technology"

948 Proactive technology may be used by regulated service providers to comply with their duties about illegal content, content which is harmful to children and fraudulent advertising. As set out in those duties, the service provider must specify in their terms of service or publicly available statement if they use proactive technology. OFCOM may recommend the use of proactive technology in the codes of practice related to these duties (see Schedule 4, Paragraph 12), and may also impose confirmation decisions requiring the use of proactive technology (see section 136). Both actions by OFCOM are subject to certain constraints included in Schedule 4 and section 136, including considering the extent to which they might result in interference with users' right to freedom of expression within the law. OFCOM can also recommend or require the use of proactive technology in relation to the Part 5duties, where necessary and proportionate.

949 This section provides a definition of proactive technology. Proactive technology consists of three types of technology for the purposes of this legislation: content identification, user profiling and behaviour identification. The section gives limited examples of the types of technologies, and makes clear that this will in some cases include artificial intelligence and machine learning technologies.

950 Content identification technology includes technology such as algorithms, keywords, image matching or image classification, which will involve, for instance, automatically analysing user-generated content across a user-to-user service for the purposes of assessing if this is illegal content. The service provider can then decide what action is required in respect of that content to comply with its safety duties about illegal content (section 10). Content identification technology is also an example of a technology that may be accredited technology in relation to the detection of terrorism content or CSEA content (see section 121). Technology which reviews content which has been flagged by a user report does not fall within this category. The restrictions on OFCOM recommending or requiring the use of proactive technology (see Schedule 4 and section 136) also apply to content identification technology operating on any kind of content.

951 User profiling technology refers to tools which build a profile of the user, assessing characteristics, so that the service provider can limit their access to harmful content if necessary. The provision notes that this will involve the analysis of content and user data, or relevant metadata of content and user data, which means this includes looking at a number of factors, such as what they post and view online, and could include data the service provider has from a partner site, for example. This includes data created by providers of all regulated services, including providers subject to the Part 5 pornography duties. It doesn't include technology that checks data (such as ID) provided by the user to verify age.

952 Behaviour identification technology is a category of technology which assesses harmful behaviour online, including criminal activity. This also concerns the analysis of content and user data, or relevant metadata of content and user data. The provision clarifies that this does not mean investigations conducted by service providers into specific users, where technology is used in response to concerns identified by another person (or another automated tool). Subsection (8) defines relevant content, which includes user-generated content, content capable of being searched in a search engine, and provider pornographic content (see 80(2)). Subsection (9) defines user data, which is a category of data which these tools will analyse in addition to content and metadata. It specifies that this will include personal data, as well as data that the service provider will create about user activity, or obtain from partner services.

Section 232: Content communicated "publicly" or "privately"

953 This section provides information to assist OFCOM in their decision making on whether content is communicated publicly or privately for the purposes of exercising its powers under the Act.

954 Subsection (1) sets out that OFCOM must consider the factors listed in this section relating to the functionality and design of the service when making decisions on whether content is communicated publicly or privately under sections 121 and 136 and under Schedule 4.

955 Subsection (2) sets out the factors that OFCOM must consider in their decision making.

956 Subsection (3) sets out the factors that OFCOM should not consider as being restrictions on users accessing a service.

Section 233: "Functionality"

957 This section sets out the meaning of the term 'functionality'.

Section 234: "Harm" etc

958 This section defines harm as physical or psychological harm. This could include physical injuries, serious anxiety and fear; longer-term conditions such as depression and stress; and medically recognised mental illnesses, both short-term and permanent.

959 It provides that harm can arise from the harmful nature of content, for example from grossly offensive, abusive or discriminatory content. It can also arise from the dissemination of content that is not by its nature harmful, for example the malicious sharing of personal information, or the way in which content is disseminated, for example one or many people repeatedly sending content to an individual.

960 Subsection (4) makes clear that references to harm in relation to content include instances where harm occurs because the user repeatedly encounters content. This would capture instances in which harm occurs due to repeated exposure to one kind of content, or a combination of different kinds of content. This may be a result of one or more users sending such content to an individual, or as a result of algorithms and other functionalities on a service repeatedly sending content to a user.

961 Subsection (5) makes provision to include indirect harm, where someone harms themself or another person as a result of content.

Section 235: "Online safety functions" and "online safety matters"

962 This section sets out the meaning of "online safety functions" and "online safety matters".

Section 236: Interpretation: general

963 This section sets out the meanings of various terms used in the Act.

Section 237: Index of defined terms

964 This section lists those provisions which define or explain terms used in the Act.

Final provisions

Section 238: Financial provisions

965 This section sets out the financial provisions for the Act.

Section 239: Extent

966 This section sets out that the Act extends to England and Wales, Scotland and Northern Ireland, subject to the provisions within this section.

967 Subsection 2 specifies the provisions that extend to England and Wales and Northern Ireland. These are: the false communications offence and exemptions from that offence, the threatening communications offence, and section 182 which deals with interpretation of those offences. It also specifies the offences of sending or showing flashing images electronically and section 189 (1) which deals with certain repeals in connection with the offences under sections 179 and 181.

968 Subsection 3 sets out the provisions which extend to England and Wales only. These are: sending etc photography or film of genitals; sending or threatening to share intimate photograph or film; section 189 (2) which deals with certain repeals in connection with the false communications and threatening communications offences; repeals in connection with the

offence of sharing or threatening to share intimate images; offence under the Obscene Publications Act 1959: OFCOM defence; and subsections (1)-(3) of section 214 - offences regarding indecent photographs of children: OFCOM defence.

969 Subsection 4 sets out which provisions extend only to Scotland. These are subsection (4)-(6) of offences regarding indecent images of children: OFCOM defence.

970 Subsection 7 provides that His Majesty may by Order in Council extend any provisions of the Act without modifications to the Crown Dependencies of the Bailiwick of Guernsey or the Isle of Man. Subsection 9 provides that section 411(6) of the Communications Act may be further exercised to extend to these two Dependencies any amendment or repeal made by or under this Act, or any part of that Act.

971 Subsection 10 to 12 make further provision regarding the exercise of powers in relation to the Bailiwick of Guernsey and the Isle of Man.

Section 240: Commencement and transitional provision

972 This section sets out when the different provisions of the Act will come into force. More details about commencement are given below.

Section 241: Short title

973 This section establishes the short title of this legislation as the Online Safety Act 2023.

Commencement

974 Section 240 provides for the commencement of the provisions in this Act.

975 Subsection (1) sets out that, except for those provisions under subsection (4), the provisions of the Act come into force on a day set out in regulations by the Secretary of State, and subsection (2) provides that different days may be appointed for different purposes.

976 Subsection (3) provides that regulations made under subsection (1) may not bring section 210 (repeal of Part 4B of the Communications Act) into force before the end of the period of six months that begins with the date that will be specified in regulations (under paragraph 8(1) of Schedule 3).

977 Subsection (4) lists the provisions that came into force on the day the Act received royal assent.

978 Subsection (5) provides that the Secretary of State may by regulations make transitional or saving provisions in connection with the coming into force of any provision of this Act. Subsection (6) sets out that the power to make regulations includes the power to make different provisions for different purposes.

979 Subsection (7) sets out that any power to make regulations under this section is exercisable by statutory instrument.

Related documents

980 The following documents are relevant to the Act and can be read at the stated locations:

- Online Harms White Paper and Consultation
- Online Harms White Paper Initial Government Response
- Online Harms White Paper Full Government Response
- Draft Online Safety Bill
- Law Commission report
- Joint Committee report on the Draft Online Safety Act
- Digital, Culture, Media and Sport Committee report
- Petitions Committee report on Online Abuse
- Online Safety Bill prints
- Impact assessment
- Delegated powers memorandum and supplementary delegated powers memorandum
- Government response to the Joint Committee report

Annex A - Territorial extent and application

981 This Act extends and applies to the whole of the UK, aside from in a small number of areas, as set out above.

982 Repeals, revocations and amendments made by the Act have the same territorial extent and application as the legislation that they are amending.

983 Regulations made under powers in the Act may have extraterritorial effect where they are being used to amend legislation which already produces a practical effect outside the UK.

984 The Act confers powers onto Devolved Ministers. These are:

a. A power for Ministers in Scotland, Wales, and the relevant department in Northern Ireland to amend the list of exempt educational institutions included at Part 2 of Schedule 1 under section 221.

b. A power for Ministers in Scotland to amend the list of CSEA offences included in Part 2 of Schedule 6 under section 222(2).

985 The Government sought the consent of the relevant legislatures for these provisions as they alter the powers of Ministers of the devolved administrations. As set out above, the Northern Ireland Assembly was adjourned during the parliamentary passage of the Act.

986 This Act also legislates for a number of new offences. The extent of these offences is set out below:

a. The False Communication Offence under sections 179, 180 and 182 extends and applies to England, Wales and Northern Ireland. It does not extend to Scotland. The offence is devolved.

b. The Threatening Communication Offence under sections 181 and 182 extends and applies to England, Wales and Northern Ireland. It does not extend to Scotland. The offence is devolved.

c. The Offence under section 183 of sending or showing flashing images electronically extends and applies to England and Wales and Northern Ireland. This offence is reserved in respect of Northern Ireland, and partially devolved for Wales. It does not extend to Scotland.

d. The Offence under section 184 of encouraging or assisting the serious self-harm of another person extends and applies to England and Wales, Scotland and Northern Ireland. This offence is devolved in respect of Wales, Scotland and Northern Ireland.

e. The Intimate Image Abuse Offence under section 187 and the Cyberflashing Offence under section 188 are to be inserted into the Sexual Offences Act 2003, which applies to England and Wales only. These offences are reserved.

Annex B - Hansard References

987 The following table sets out the dates and Hansard references for each stage of the Act's passage through Parliament.

Stage	Date	Hansard Reference
House of Commons		
Introduction	17 March 2022	Vol. 710 Col. 1092
Second Reading	19 April 2022	Vol. 712 Col. 93
Public Act Committee	24 May 2022 24 May 2022 26 May 2022 26 May 2022 7 June 2022 7 June 2022 9 June 2022 9 June 2022 14 June 2022 14 June 2022 16 June 2022 16 June 2022 21 June 2022 21 June 2022 23 June 2022 28 June 2022 28 June 2022 *Following Re-Committed clauses and Schedule:* 13 December 2022 13 December 2022	1st Sitting 2nd Sitting 3rd Sitting 4th Sitting 5th Sitting 6th Sitting 7th Sitting 8th Sitting 9th Sitting 10th Sitting 11th Sitting 12th Sitting 13th Sitting 14th Sitting 15th Sitting 16th Sitting 17th Sitting 1st Sitting 2nd Sitting

	15 December 2022	3rd Sitting
Report and Third Reading	12 July 2022 5 December 2022 17 January 2023 17 January 2023	Vol. 718 Col. 147 Vol. 724 Col. 22 (re-committal) Vol. 726 Col. 266 Vol. 726, Col. 266
House of Lords		
Introduction	18 January 2023	Vol. 826 Col. 1825
Second Reading	01 February 2023	Vol. 827 Col. 686
Grand Committee	19 April 2023 25 April 2023 25 April 2023 27 April 2023 27 April 2023 2 May 2023 2 May 2023 9 May 2023 9 May 2023 11 May 2023 16 May 2023 16 May 2023 23 May 2023 23 May 2023 25 May 2023 22 June 2023 22 June 2023	Vol. 829 Col. 698 Vol. 829 Col. 1112 Vol. 829 Col. 1185 Vol. 829 Col. 1286 Vol. 829 Col. 1330 Vol. 829 Col. 1421 Vol. 829 Col. 1481 Vol. 829 Col. 1681 Vol. 829 Col. 1739 Vol. 829 Col. 1996 Vol. 830 Col. 134 Vol. 830 Col. 219 Vol. 830 Col. 764 Vol. 830 Col. 839 Vol. 830 Col. 989 Vol. 831 Col. 336 Vol. 831 Col. 385
Report	06 July 2023 06 July 2023	Vol. 831 Col. 1319 Vol. 831 Col. 1363

	06 July 2023 10 July 2023 10 July 2023 12 July 2023 17 July 2023 19 July 2023	Vol. 831 Col. 1413 Vol. 831 Col. 1529 Vol. 831 Col. 1612 Vol. 831 Col. 1744 Vol. 831 Col. 2037 Vol. 831 Col. 2327
Third Reading	06 September 2023	Vol. 832 Col. 447
Commons Consideration of Lords Amendments	12 September 2023	Vol. 737 Col. 799
Lords' Consideration of Commons Amendments	19 September 2023	Vol. 832 Col.1339
Royal Assent	26 October 2023	House of Commons Vol. 738 Col. 999 House of Lords Vol. 833 Col. 695

Annex C - Progress of Bill Table

988 This Annex shows how each section and Schedule of the Act was numbered during the passage of the Bill through Parliament.

Section of the Act	Bill as Introduced in the Commons	Bill as amended in Committee in the Commons	Bill as introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords
1					1
2	1	1	1	1	2
3	2	2	2	2	3
4	3	3	3	3	4
5	4	4	4	4	5
6	5	5	5	5	6
7	6	6	6	6	7
8	7	7	7	7	8
9	8	8	8	8	9
10	9	9	9	9	10
11	10	10	10	10	11
12	11 (the following sections were removed: Section 12 (adult's risk assessment duties); and 13 (safety duties protecting adults)	11 (the following sections were removed: Section 12 (adult's risk assessment duties); and 13 (safety duties protecting adults)	11	11	12
13					13
14					14
15	14	14	12	12	15
16					16
17			13	13	17
18	15	15	14	14	18
19	16	16	15	15	19
20	17	17	16	16	20
21	18	18	17	17	21

22	19	19	18	18	22
23	20	20	19	19	23
24	21	21	20	20	24
25	22	22	21	21	25
26	23	23	22	22	26
27	24	24	23	23	27
28	25	25	24	24	28
29	26	26	25	25	29
30					30
31	27	27	26	26	31
32	28	28	27	27	32
33	29	29	28	28	33
34	30	30	29	29	34
35	31	31	30	30	35
36	32	32	31	31	36
37	33	33	32	32	37
38	34	34	33	33	38
39	35	35	34	34	39
40	36	36	35	35	40
41	37	37	36	36	41
42	38	38	37	37	42
43	39	39	38	38	43
44	40	40	39	39	44
45	41 (was section 40)	41 (was section 40)	40 (was section 39)	40 (was section 39)	45
46	42	42	41	41	46
47	43	43	42	42	47
48	44	44	43	43	48
49	45	45	44	44	49
50	46	46	45	45	50
51	47	47	46	46	51

52	48 (was OFCOM's guidance: record-keeping duties and children's access assessments)	48 (was OFCOM's guidance: record-keeping duties and children's access assessments)	47	47	52
53			48	48	53
54					54
55	49	49	49	49	55
56	50	50	50	50	56
57			51	51	57
58	51	51	52	52	58
59	52	52	53	53	59
60	53	53	54	54	60
61					61
62					62
63	55 (was 57: Regulations under section 53; and 54: OFCOM's review and report)	55 (was 57: Regulations under section 53; and 54: OFCOM's review and report)	56 (was 55: Regulations under section 54; and 56: OFCOM's review and report)	56 (was 55: Regulations under section 54; and 56: OFCOM's review and report)	63
N/A					64
64	57	57	57	57	65
65	58	58	58	58	66
66	59	59	59	59	67
67	60	60	60	60	68
68	61	61	61	61	69
69	62	62	62	62	70
70	63	63	63	63	71
71			64	64	72
72			65	65	73
73			66	66	74
74			67	67	75
75					76
76					77

77	64	64	68	68	78
78	65	65	69	69	79
79	66	66	70	70	80
80	67	67	71	71	81
81	68	68	72	72	82
82	69	69	73	73	83
83	70	70	74	74	84
84	71	71	75	75	85
85	72 (was: OFCOM's statement about "qualifying worldwide revenue")	72 (was: OFCOM's statement about "qualifying worldwide revenue")	76 (was: OFCOM's statement about "qualifying worldwide revenue")	76 (was: OFCOM's statement about "qualifying worldwide revenue")	86
86	73	73	77	77	87
87	74	74	78	78	88
88	75	75	79	79	89
89		76	80	80	90
90	76	77	81	81	91
91	77	78	82	82	92
92	78	79	83	83	93
93	79	80	84	84	94
94	80	81	85	85	95
95	81	82	86	86	96
96	82	83	87	87	97
97			88	88	98
98	83	84	89	89	99
99	84	85	90	90	100
100	85	86	91	91	101
101					102
102	86	87	92	92	103
103	87	88	93	93	104
104	88	89	94	94	105

105	89	90	95	95	106
106	90	91	96	96	107
107	91	92	97	97	108
108				98	109
109	92	93	98	99	110
110	93	94	99	100	111
111	94	95	100	101	112
112	95	96	101	102	113
113	96	97	102	103	114
114	97	98	103	104	115
115	98	99	104	105	116
116	99	100	105	106	117
117	100	101	106	107	118
118			107	108	119
119	101	102	108	109	120
120	102	103	109	110	121
121	103	104	110	111	122
122					123
123			111	112	124
124	104	105 (was section 104(1))	112 (was section 110(1))	113 (was section 111(1))	125
125	105	106 (was section 104(1))	113 (was section 110(1))	114 (was section 111(1))	126
126	106	107 (was section 104(1))	114	115	127
127	107	108	115	116	128
128	108	109	116	117	129
129	109	110	117	118	130
130	110	111	118	119	131
131	111	112	119	120	132
132	112	113	120	121	133

133	113	114	121	122	134
134	114	115	122	123	135
135	115	116	123	124	136
136	116	117	124	125	137
137	117	118	125	126	138
138				127	139
139	118	119	126	128	140
140	119	120 (was section 104(1))	127 (was section 110(1))	129 (was section 111(1))	141
141	120	121	128	130	142
142	121 (was sections 199 and 120)	122 (was sections 120 and 121)	129 (was sections 127 and 128)	131 (was sections 129 and 130)	143
143	122	123	130	132	144
144	123	124	131	133	145
145	124	125	132	134	146
146	125	126	133	135	147
147	126	127	134	136	148
148	127	128	135	137	149
149	128 (formerly Publication of details of enforcement actions)		136	138	150
150		129	137	139	151
151	129	130	138	140	152
152	130	131	139	141	153
153	131	132	140	142	154
154	132	133	141	143	155
155	133	134	142	144	156
156	134	135	143	145	157
157					158
158	135		144	146	159
159	136	136	145	147	160
160					161

161					162
162		137	146	148	163
163					164
164	137	138	147	149	165
165					166
166					167
167	138 (was section 81)	139 (was section 82)	148	150	168
168	139	140	149	151	169
169	140	141	150	152	170
170	141	142	151	153	171
171	142	143	152	154	172
172	143	144	153	155	173
173	144	145	154	156	174
174	145	146	155	157	175
175	146	147	156	158	176
176	147	148	157	159	177
177	148	149	158	160	178
178	149 (clause 150: Harmful Communications offence removed)	150	159	161	179
179	151		160	162	180
180			161 (was section 160)	163 (was section 162)	181
181	152		162	164	182
182	153 (was sections 150 and 152)		163 (was sections 160 to 162)	165 (was sections 162 to 164)	183
183			164	166	184
184			165	167	185
185	154		166	168	186
186	155		166	169	187
187	156		167	170	188
188					189

189	157 (was sections 150, 151 and 152)	158 (was sections 151, 152 and 153)	168 (was section 160 and 162)	171 (was section 162 and 164)	190
190					191
191	158	159	169	172	192
192			170	173	193
193			171	174	194
194					195
195	159	160	172	175	196
196	160	161	173	176	197
197	161	162	174	177	198
198			175	178	199
199	162	163	176	179	200
200				180	201
201	163	164	177	181	202
202	164	165	178	182	203
203	165	166	179	183	204
204	166	167	180	184	205
205	167 (formerly: Information offences: extra-territorial and jurisdiction)	168	181	185	206
206		169	182	186	207
207	168	170	183	187	208
208	169	171	184	188	209
209			185	198	210
210	170	172	186	190	211
211			187	191	212
212	171	173	188	192	213
213		174	189	193	214
214	172	175	190	194	215
215					216
216					217

217					218
218	173 (was section 36)	176 (was section 36)	191 (was section 35)	195 (was section 35)	219
219					220
220	174	177	192	196	221
221	175	178	193	197	222
222	176	179	194	198	223
223	177	180	195	199	224
224	178	181	196	200	225
225	179	182	197	201	226
226	180	193	198	202	227
227	181	184	199	203	228
228	182	185	200	204	229
229	183	186	201	205	230
230					231
231	184	187	202	206	232
232	185	188	203	207	233
233	186	189	204	208	234
234	187	190	205	209	235
235	188	191	206	210	236
236	189	192	207	211	237
237	189	193	208	212	238
238	191	194	209	213	239
239	192	195	210	214	240
240	193	196	211	215	241
241	194	197	212	216	242
Schedule 1	Schedule 1	Schedule 1	Schedule 1	Schedule 1	Schedule 1
Schedule 2	Schedule 2	Schedule 2	Schedule 2	Schedule 2	Schedule 2
Schedule 3	Schedule 3	Schedule 3	Schedule 3	Schedule 3	Schedule 3
Schedule 4	Schedule 4	Schedule 4	Schedule 4	Schedule 4	Schedule 4
Schedule 5	Schedule 5	Schedule 5	Schedule 5	Schedule 5	Schedule 5

Schedule 6	Schedule 6	Schedule 6	Schedule 6	Schedule 6	Schedule 6
Schedule 7	Schedule 7	Schedule 7	Schedule 7	Schedule 7	Schedule 7
Schedule 8	Schedule 8	Schedule 8	Schedule 8	Schedule 8	Schedule 8
Schedule 9	Schedule 9	Schedule 9	Schedule 9	Schedule 9	Schedule 9
Schedule 10	Schedule 10	Schedule 10	Schedule 10	Schedule 10	Schedule 10
Schedule 11	Schedule 11	Schedule 11	Schedule 11	Schedule 11	Schedule 11
Schedule 12	Schedule 12	Schedule 12	Schedule 12	Schedule 12	Schedule 12
Schedule 13	Schedule 13	Schedule 13	Schedule 13	Schedule 13	Schedule 13
Schedule 14	Schedule 14	Schedule 14	Schedule 14	Schedule 14	Schedule 14
Schedule 15		Schedule 15	Schedule 15	Schedule 15	Schedule 15
Schedule 16			Schedule 16	Schedule 16	Schedule 16
Schedule 17			Schedule 17	Schedule 17	Schedule 17

Printed and published in the UK by The Stationery Office Limited under the authority and superintendence of Jeff James, Controller of His Majesty's Stationery Office and King's Printer of Acts of Parliament.