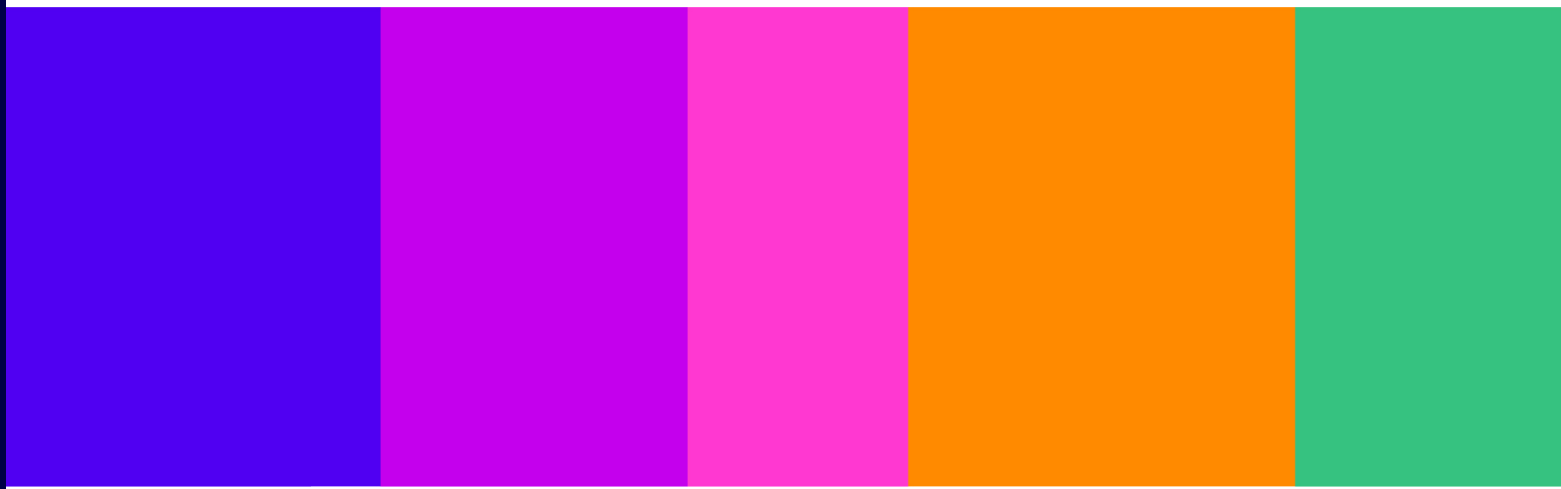


Protecting people from illegal harms online

Annex 2: Legal Framework Overview (Part A)
and Duties of Providers and Ofcom in
relation to illegal content (Part B)

Annexe

Published 16 December 2024



Contents

Section

A2	Legal Framework Overview (Part A).....	3
	Introduction	3
	The Online Safety Act 2023	3
A2	Duties of Providers and Ofcom in relation to illegal content (Part B)	12
	Provider duties in relation to illegal content.....	12
	Providers of U2U services	12
	Illegal Content Duties	13
	Duties about content reporting and complaints procedures.....	16
	Cross-cutting duties	18
	Providers of search services	20
	Ofcom’s duties in relation to illegal content	25

A2 Legal Framework Overview (Part A)

Introduction

- A2.1 This Annex is in two sections. This first section sets out parts of the legal and regulatory framework under the Online Safety Act 2023 ('the Act') that are relevant to this Statement. It is intended to provide a high-level summary as context for our Statement but is not a comprehensive outline of service providers' obligations under the Act. It focuses on the duties the Act places on Ofcom and online service providers in relation to illegal content in particular, and we have not referred to aspects of the legal and regulatory framework which relate to the protection of children, which will be covered in our later Statement due to be published in 2025. You can find the full text of the Act here.¹
- A2.2 The second section of this Annex sets out Ofcom's and providers' duties relating to illegal content in more detail.
- A2.3 The Act places a number of duties on Ofcom and the online services who fall within scope of the new regime, namely user-to-user, search and pornography services. This Statement focuses on the first two categories of services.

The Online Safety Act 2023

Overview of the Act

Scope

- A2.4 The Act provides for a new regulatory framework which has the general purpose of making the use of regulated internet services safer for individuals in the UK. To achieve this, the Act imposes duties which require providers to identify, mitigate and manage the risks of harm from illegal content and activity and content and activity that is harmful to children, as well as conferring new functions and powers on Ofcom. Duties imposed on providers seek to secure, among other things, that regulated services are safe by design.²
- A2.5 Internet services within scope of the new regulatory regime can be broadly grouped as:
- a) a "user-to-user service", which means an internet service through which content that is generated, uploaded or shared by users may be encountered by other users of the service;³
 - b) a "search service", which means an internet service that is, or includes, a search engine;⁴
or

¹ Online Safety Act 2023. <https://www.legislation.gov.uk/ukpga/2023/50>, [accessed 2 September 2024].

² Section 1 of the Act.

³ Section 3(1) of the Act.

⁴ Section 3(4) of the Act.

- c) a provider of internet services on which “provider pornographic content” is published or displayed.⁵
- A2.6 Such services will only be in scope if they have “links to the United Kingdom”⁶ and do not fall within Schedule 1 (exempt services). Regulated services have links to the UK if the service has a significant number of UK users or if UK users form one of the target markets or the only target market.⁷ A service will also be considered to have links to the UK if it is capable of being used in the UK by individuals, and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK presented by user-generated content present on the service or search content of the service.⁸
- A2.7 The Act establishes categories of regulated user-to-user and search services. Category 1 and Category 2B relate to different kinds of regulated user-to-user services, with Category 1 being the largest services. Category 2A relates to search services. The Secretary of State is responsible for setting threshold conditions for these categories based on the number of users of the service, its functionalities and other relevant factors.⁹ Once the threshold conditions have been set, Ofcom is required to maintain and publish a register of the services in each category.¹⁰
- A2.8 Please see our Overview of regulated services chapter for further discussion of these provisions.

Provider duties

- A2.9 The Act places duties of care (Part 3) and other duties (Part 4) on all providers of user-to-user services and search services. These include requirements to:
- a) for user-to-user and search services:
- i) carry out a suitable and sufficient illegal content risk assessment;¹¹
 - ii) put in place systems and processes which allow users and affected persons to easily report illegal content and content that is harmful to children to the service provider;¹²
 - iii) operate a transparent and easy to use and access complaints procedure which allows for complaints of specified types to be made, including about illegal content;¹³
 - iv) have particular regard to the importance of protecting users’ right to freedom of expression within the law, and protecting users from a breach of privacy, when deciding on and implementing safety measures and policies;¹⁴
 - v) put in place systems and processes designed to ensure that detected and unreported CSEA content is reported to the NCA.¹⁵

⁵ Section 79 of the Act.

⁶ Section 4(2)(a) of the Act,

⁷ Section 4(5) of the Act.

⁸ Section 4(6) of the Act.

⁹ Schedule 11 of the Act.

¹⁰ Section 95 of the Act.

¹¹ Sections 9 and 26 of the Act.

¹² Sections 20 and 31 of the Act.

¹³ Sections 21 and 32 of the Act.

¹⁴ Sections 22 and 33 of the Act.

¹⁵ Section 66 of the Act.

- b) for user-to-user services only:¹⁶
 - i) take or use proportionate measures to prevent individuals from encountering priority illegal content; effectively mitigate and manage the risk of the service being used for the commission or facilitation of a priority offence; and effectively mitigate and manage the risks of harm to individuals as identified in a service's most recent illegal content risk assessment; and
 - ii) use proportionate systems and processes designed to minimise the length of time for which any priority illegal content is present and to swiftly take down illegal content when the provider becomes aware of it;
 - iii) explain in clear and accessible terms of service how the service is protecting its users from illegal content and apply these terms of service consistently;
- c) for search services only:¹⁷
 - i) take or use proportionate measures to effectively mitigate and manage the risks of harm to individuals as identified in a service's most recent illegal content risk assessment;
 - ii) use proportionate systems and processes designed to minimise the risk of individuals encountering priority illegal content and other illegal content that the provider knows about;
 - iii) explain in clear and accessible provisions in a public statement how individuals are to be protected from search content that is illegal content, and apply those provisions consistently;
- d) for user-to-user services and search services likely to be accessed by children:
 - i) carry out a suitable and sufficient children's risk assessment in accordance with Schedule 3 and keep it up to date;¹⁸
 - ii) take or use proportionate measures to effectively mitigate and manage the risks of harm to children in different age groups as identified in a service's most recent children's risk assessment, and mitigate the impact of harm to children in different age groups presented by content that is harmful to children;¹⁹
- e) in addition, user-to-user services likely to be accessed by children must notify Ofcom where a children's risk assessment identifies the presence of non-designated content that is harmful to children;²⁰ and operate the service using proportionate systems and processes designed to prevent children of any age from encountering primary priority content that is harmful to children and protect children in age groups judged at risk of harm from encountering other content that is harmful to children;²¹
- f) search services likely to be accessed by children must also use proportionate systems and processes designed to minimise the risk of children of any age encountering primary priority content that is harmful to children, and minimise the risk of children in age groups judged to be at risk of harm from other content that is harmful to children.²²

¹⁶ Section 10 of the Act.

¹⁷ Section 27 of the Act.

¹⁸ Sections 11 and 28 of the Act.

¹⁹ Sections 12(2) and 29(2) of the Act.

²⁰ Section 11(5) of the Act.

²¹ Section 12(3) of the Act.

²² Section 29(3) of the Act.

- A2.10 In relation to illegal content, the Act defines this as “content that amounts to a relevant offence”.²³ A relevant offence refers to a priority offence (terrorism offences,²⁴ offences related to child sexual exploitation or abuse²⁵ or other priority offences as specified in Schedule 7) or any other type of offence where the victim is an individual or individuals,²⁶ subject to certain exceptions.²⁷
- A2.11 Please see our Overview of Illegal Harms chapter for further discussion of these duties.
- A2.12 Providers of Category 1 services are also subject to a number of additional duties, including requirements to abide by their terms of service and apply them consistently.²⁸ The Act also places specific duties on services in relation to certain pornographic content²⁹ and fees.³⁰ Volume 2 Chapter 1 of this Statement deals with terms of service for providers of Category 1 services. The other duties will be dealt with in different decisions.

Ofcom’s Codes of Practice and guidance

- A2.13 Ofcom must issue Codes of Practice for regulated user to user and search services containing measures recommended for the purposes of compliance with certain duties referred to above, including the illegal content safety duties in sections 10 and 27.³¹ In preparing these Codes of Practice, Ofcom must consider the principles and objectives set out Schedule 4 to the Act. Please see Volume 2 Chapter 14 for further discussion of these requirements.
- A2.14 Where a Code of Practice exists, a provider of a regulated user-to-user service is to be treated as complying with a relevant duty if the provider takes or uses the measures described in the Code of Practice which are recommended for the purpose of complying with that duty (this is sometimes referred to as a “safe harbour”). In addition, providers are treated as complying with the cross-cutting duties regarding freedom of expression and privacy set out in sections 22 and 33 if they take or use such of the relevant recommended measures as incorporate safeguards to protect users’ rights to freedom of expression and privacy. Providers may choose to take alternative measures to comply with the relevant duties rather than following the recommended measures in Codes.³²
- A2.15 Ofcom is further required to issue Illegal Content Judgements Guidance.³³

Ofcom’s duties relating to risk

- A2.16 Ofcom must carry out risk assessments to identify and assess the risks of harm to individuals in the UK presented by:
- a) illegal content on user-to-user services and the use of such services for the commission or facilitation of priority offences; and
 - b) illegal content that is search content encountered on search services.³⁴

²³ Section 59(2) of the Act.

²⁴ Schedule 5 of the Act.

²⁵ Schedule 6 of the Act.

²⁶ Section 59(5) of the Act.

²⁷ Section 59(6) of the Act.

²⁸ Sections 71 and 72 of the Act.

²⁹ Part 5 of the Act.

³⁰ Part 6 of the Act.

³¹ Section 41 of the Act.

³² Section 49 of the Act.

³³ Section 193 of the Act.

³⁴ Section 98(1) of the Act.

- A2.17 Ofcom must also carry out a risk assessment to identify and assess the risk of harm presented by user-to-user and search services to children in the UK, in different age groups, by content that is harmful to children.³⁵
- A2.18 We must also prepare and publish a Register of Risks that reflects the findings of our risk assessments³⁶ as well as Risk Profiles for user-to-user services and search services that relate to each risk of harm.³⁷
- A2.19 Ofcom is also required to issue guidance relating to how providers can comply with the risk assessment duties.³⁸
- A2.20 Please see Volume 1 Chapter 3 for further discussion of these duties.

Information gathering and enforcement

- A2.21 The Act gives Ofcom broad powers regarding information gathering for the purposes of discharging our functions, including powers:
- a) to require information generally from providers (by notice) for the purposes of exercising, or deciding whether to exercise, functions;³⁹
 - b) to appoint a skilled person to provide a report to Ofcom for certain purposes relating to compliance;⁴⁰
 - c) to require certain individuals to attend interviews and answer questions;⁴¹ and
 - d) of entry, inspection and audit.⁴²
- A2.22 Ofcom is responsible for enforcing compliance with the duties in the Act on providers of regulated services. The duties on providers are generally enforceable by Ofcom where there are reasonable grounds for believing that a provider has failed, or is failing, to comply.⁴³
- A2.23 Sanctions for non-compliance may include requiring payment of a financial penalty of up to £18m or 10% of qualifying worldwide revenue.⁴⁴ In certain circumstances, Ofcom may apply to a court to take business disruption measures against platforms.⁴⁵ Ofcom may also, if certain conditions are met, issue notices requiring providers to use accredited technology or to develop or source technology to prevent users from encountering, or to identify and take down, terrorism content that is communicated publicly or CSEA content that is communicated publicly or privately.⁴⁶
- A2.24 Part 8 of the Act relates to appeals against Ofcom’s decisions about the register under section 95 of the Act (regarding categorisation of services) and against Ofcom notices, while Part 9 relates to the Secretary of State’s functions in respect of regulated services.

³⁵ Section 98(1) of the Act.

³⁶ Section 98(4) of the Act.

³⁷ Section 98(5) of the Act.

³⁸ Section 99 of the Act.

³⁹ Section 100 of the Act.

⁴⁰ Section 104 of the Act.

⁴¹ Section 106 of the Act.

⁴² Section 107 of the Act.

⁴³ Section 130 of the Act.

⁴⁴ Schedule 13 of the Act.

⁴⁵ See sections 144 to 148 of the Act.

⁴⁶ Section 121 of the Act.

- A2.25 Part 10 of the Act creates various new communications offences, some of which we refer to in our regulatory outputs. These offences include false and threatening communications offences and the offence of sending photographs or films of genitals.
- A2.26 Further detail on the duties in the Act that are relevant to our statement is contained in the second section of this Annex.

The process for making Codes of Practice and guidance

Codes of Practice

- A2.27 The Act specifies the procedure which applies to Ofcom when issuing, or amending, Codes of Practice.
- A2.28 In the course of preparing a draft Code of Practice, Ofcom must consult various persons specified in section 41(6) and 41(7) of the Act. These include the Secretary of State; persons who represent services and their users; persons who represent the interests of children and those who have suffered harm as a result of matters to which the Codes relate; persons with expertise in equality issues, human rights, public health, criminal law enforcement, national security, innovation and emerging technology; and other public bodies such as the Information Commissioner and the Children’s Commissioner, Domestic Abuse Commissioner and Commissioner for Victims and Witnesses.
- A2.29 Once Ofcom has prepared a draft Code (or draft amendments to a Code), we must submit it to the Secretary of State.⁴⁷ The Secretary of State must either issue a direction under section 44 of the Act or lay the draft before Parliament. If either House of Parliament resolves not to approve the draft Code within the 40-day period,⁴⁸ Ofcom cannot issue that draft Code and must prepare another draft. If no such resolution is made, Ofcom must issue the draft Code in that form and it will come into force 21 days later.⁴⁹
- A2.30 The Secretary of State may direct Ofcom to modify a draft Code for exceptional reasons relating to national security, public health or safety or foreign relations or, in the case of a terrorism or CSEA Code, for reasons of national security, public health or safety or exceptional reasons relating to foreign relations.⁵⁰ If a draft terrorism or CSEA Code has been the subject of a review under section 47(2), or Ofcom has submitted a statement to the Secretary of State under section 47(3)(b) in respect of such a Code, the Secretary of State can only issue a direction to modify the draft for reasons of national security or public safety. A direction given under section 44 cannot require Ofcom to include any particular measure in a Code and must set out the Secretary of State’s reasons for requiring modifications (unless it would be against the interests of national security, public safety or relations with the government of a country outside the UK i.e. foreign relations). Ofcom must comply with any direction and submit a revised Code as soon as reasonably practicable. When the Secretary of State is satisfied that no further modifications to the draft are required, the draft must be laid before Parliament.
- A2.31 If a draft Code has been laid before Parliament following a direction and modifications under section 44(1), (2) or 3(b) of the Act then the affirmative procedure applies.⁵¹ If a draft

⁴⁷ Section 43 of the Act.

⁴⁸ See sections 45(5) and (6) of the Act.

⁴⁹ See section 45(4) of the Act.

⁵⁰ Section 44 of the Act.

⁵¹ Which is set out in section 45(4) of the Act.

terrorism or CSEA Code has been the subject of a direction and modifications under section 44(3)(a), (4) or (5) then the negative procedure applies.⁵²

- A2.32 Ofcom must publish each Code (or amendments to a Code) within three days of when it is issued.⁵³ Where we withdraw a Code of Practice, we must publish a notice to that effect.⁵⁴
- A2.33 We must keep each Code we publish under review.⁵⁵ The Secretary of State can require us to review a terrorism or CSEA Code for reasons of national security or public safety, and we must carry out such a review as soon as reasonably practicable. We must then make any necessary changes to the Code, or if we consider no changes are required, submit a statement to the Secretary of State explaining why.⁵⁶
- A2.34 Subject to the Secretary of State's approval, Ofcom may make minor amendments to a Code without consultation or laying the amendments before Parliament.⁵⁷
- A2.35 The safety duties apply to providers from the day on which the first relevant Code comes into force.⁵⁸

Guidance

- A2.36 The Act sets out various procedural requirements relating to the other forms of guidance that Ofcom is required to produce.
- A2.37 In relation to the Illegal Content Judgements Guidance,⁵⁹ Ofcom is required to consult before producing the guidance (or revised or replacement guidance) and publish the guidance.
- A2.38 Ofcom must also publish the Risk Profiles prepared under section 98 and from time to time review and revise the risk assessments and Risk Profiles so as to keep them up to date. Ofcom is further required to consult the Information Commissioner before producing our guidance (or revised or replacement guidance) about risk assessments under section 99. We must revise this guidance from time to time in response to further risk assessments under section 98 or to revisions of the Risk Profiles. Ofcom must publish this guidance.
- A2.39 Under section 52, Ofcom must produce guidance for providers to assist them in complying with their duties set out in sections 23 or 34 regarding record-keeping and review and section 36 regarding children's access assessments. Ofcom must also produce guidance for Category 1 services relating to their duties set out in section 14 (assessments related to the adult user empowerment duty set out in section 15(2)) and section 18 (news publisher content). Ofcom must consult the Information Commissioner before producing this guidance (except for the news publisher content guidance) and publish the guidance.
- A2.40 In relation to Ofcom's guidance about enforcement action,⁶⁰ we must consult the Secretary of State, the Information Commissioner and such other persons we consider appropriate

⁵² Which is set out in section 45(5) of the Act.

⁵³ Section 46 of the Act.

⁵⁴ Section 46(3) of the Act.

⁵⁵ Section 47 of the Act.

⁵⁶ Section 47(3) of the Act.

⁵⁷ Section 48 of the Act.

⁵⁸ Section 51 of the Act.

⁵⁹ Section 193 of the Act.

⁶⁰ Section 151 of the Act.

before producing the guidance (or revised or replacement guidance) and publish the guidance.

- A2.41 Schedule 13 refers to Ofcom’s penalty guidelines issued under s. 392 of the CA 2003 insofar as they are relevant to penalties imposed under the Act. Ofcom must consult on these guidelines, in particular the Secretary of State, and publish the guidelines in a way we consider appropriate for bringing them to the attention of persons who are likely to be affected by them. The penalty guidelines may be included in the same document as the enforcement guidance.⁶¹

Impact assessments

- A2.42 Impact assessments provide a valuable way of assessing the options for regulation and showing why the chosen option(s) was preferred. They form part of best practice policy making. This is reflected in section 7 of the CA 2003,⁶² which means that Ofcom generally must carry out impact assessments in cases where it appears to us our proposals are important. Proposals that are important for the purposes of this section include preparing (or amending) a Code of Practice under section 41 of the Act; proposals which would be likely to have a significant effect on businesses or the general public; or where there is a major change in Ofcom’s activities. As a matter of policy, Ofcom is committed to carrying out impact assessments in the great majority of our policy decisions. Our impact assessment guidance sets out our general approach to how we assess and present the impact of our proposed decisions.⁶³
- A2.43 As set out in section 7(5) of the CA 2003, Ofcom has discretion as to the substance and form of an impact assessment, and this will depend on the particular proposals being made. However, impact assessments which relate to proposals about Codes specifically or anything else for the purposes of the carrying out of Ofcom’s online safety functions under the Act must include an assessment of the likely impact of implementing the proposal on small and micro businesses.⁶⁴

Other relevant powers and duties

- A2.44 There are several other duties in the Act which are relevant to the proposals covered in this consultation.
- A2.45 As referred to above, section 66 contains a requirement to report CSEA content to the NCA. Specifically, this section requires:
- a) a UK provider of user-to-user services to use systems and processes which secure (so far as possible) that the provider reports all detected and unreported CSEA content present on the service to the NCA (a non-UK provider of a user-to-user service must only do so in relation to UK-linked CSEA content); and
 - b) a UK provider of a search service to use systems and processes which secure (so far as possible) that the provider reports all detected and unreported CSEA content present on websites or databases capable of being searched by the search engine to the NCA (a

⁶¹ Section 151(6) of the Act.

⁶² As amended by section 93 of the Act.

⁶³ Ofcom, 2023, [Impact assessment guidance](#). [accessed 4 September 2024].

⁶⁴ Section 93 of the Act.

non-UK provider of a search service must only do so in relation to UK-linked CSEA content).

- A2.46 The duties on providers of search services apply to providers of combined services in relation to the search engine of the service. Providers' reports under this section must meet the requirements set out in regulations made by the Secretary of State under section 67 of the Act, including in relation to time frames.
- A2.47 Section 64 of the Act contains requirements relating to user identity verification. Providers of Category 1 services must offer all adult users of the service in the UK the option to verify their identity. The provider must also include clear and accessible provisions in the terms of service explaining how the verification process works. Ofcom must issue guidance for providers of Category 1 services to assist them in complying with this duty.⁶⁵

⁶⁵ Section 65 of the Act.

A2 Duties of Providers and Ofcom in relation to illegal content (Part B)

- A2.1 This part of this Annex sets out in more detail the duties relating to illegal harms, as they apply to providers of user-to-user services ('U2U services'); providers of search services; and to Ofcom, and which are relevant to this statement.
- A2.2 This Annex does not cover other duties set out in the Act (except where relevant to illegal harms). Therefore, duties relating to, for example, the protection of children; user empowerment; the protection of content of democratic importance, news publisher content or journalistic content; fraudulent advertising; and other provisions of the Act are outside the scope of this statement and will be addressed separately.⁶⁶

Provider duties in relation to illegal content

- A2.3 As summarised in paragraphs A2.9-2.12, the Act imposes "duties of care" on providers of regulated user-to-user services ('U2U services'); and providers of regulated search services in relation to, among other things, "illegal content" (defined under section 59 of the Act. See also Chapter 2 of this consultation). Under the Act, "illegal content" is defined as "content that amounts to a relevant offence".⁶⁷ For U2U services, some of the duties apply in relation to the use of the service in question for the commission or facilitation of the defined priority offences identified in the Act (see paragraphs 1.24-28 of the Overview of Illegal Harms chapter).
- A2.4 The duties in relation to illegal content are set out in detail below.

Providers of U2U services

- A2.5 Providers of U2U services are given specific duties under the Act in relation to illegal content. These "Illegal content duties" include: "Illegal content risk assessment duties";⁶⁸ and "Safety duties about illegal content".⁶⁹
- A2.6 Providers of U2U services are also subject to "additional duties" which are relevant, among other things, to illegal content. These additional duties are as follows:
- a) "Duties about content reporting and complaints procedures", which include:
 - i) "Duties about content reporting",⁷⁰ and
 - ii) "Duties about complaints procedures"⁷¹ and

⁶⁶ For further information about how we are implementing the Online Safety Act, see [Implementing the Online Safety Act: Progress Update \(17 October 2024\)](#). [accessed 25 October 2024].

⁶⁷ Section 59 of the Act.

⁶⁸ Section 9 of the Act.

⁶⁹ Section 10 of the Act.

⁷⁰ Section 20 of the Act.

⁷¹ Section 21 of the Act.

- b) so-called “Cross-cutting duties”, which include:
 - iii) “Duties about freedom of expression and privacy”;⁷² and
 - iv) “Record-keeping and review duties”.⁷³

A2.7 These are set out in more detail below. Section 7 of the Act states that all providers of regulated U2U services must comply with these duties (and the other duties set out under section 7(2)).

Risk assessment requirement

A2.8 These duties only apply to:

- a) the design, operation and use of the service in the United Kingdom, and
- b) in the case of a duty that is expressed to apply in relation to users of a service, the design, operation and use of the service as it affects United Kingdom users of the service.⁷⁴

Combined services

A2.9 Where the U2U service is a combined service (i.e. providing both a regulated U2U and regulated search service), these duties will not apply to:

- a) the search content of the service,
- b) any other content that, following a search request, may be encountered as a result of subsequent interactions with internet services, or
- c) anything relating to the design, operation or use of the search engine.⁷⁵

A2.10 However, the duties of care that apply to regulated search services in relation to illegal content (see paragraphs A2.39-59 below), will still apply.

Illegal Content Duties

Illegal content risk assessment duties

A2.11 Providers of regulated U2U services have a duty to carry out a suitable and sufficient illegal content risk assessment⁷⁶ at the specific times set out in Schedule 3 to the Act.⁷⁷

⁷² Section 22 of the Act.

⁷³ Section 23 of the Act.

⁷⁴ Section 8(3) of the Act.

⁷⁵ Section 8(2) of the Act.

⁷⁶ Section 9(2) of the Act.

⁷⁷ The deadline for completing the first risk assessment depends on the day on which a provider of U2U services starts its operations. In particular:

- i. U2U services that are already in operation at the outset of this regime, must complete their first illegal content risk assessment within a period of three months from the day on which Ofcom’s risk assessment guidance (‘RAG’) is published;
- ii. new U2U services that start operations after the RAG is published must complete their first illegal content risk assessment within a period of three months from the day on which they begin their new service; and
- iii. existing services that become U2U services (having previously provided a different type of service) after the RAG is published must complete their first illegal content risk assessment within a period of three months from the day on which their service becomes a U2U service. See Schedule 3 to the Act.

- A2.12 An illegal content risk assessment means an assessment of the following matters, taking into account the risk profiles that relate to the services of that kind:⁷⁸
- a) user base;
 - b) the level of risk of individuals who are users of the service encountering, by means of the service, (i) each kind of priority illegal content (with each kind separately assessed) and (ii) other illegal content, taking into account (in particular) algorithms used by the service, and how easily, quickly and widely content may be disseminated by means of the service;
 - c) the level of risk of the service being used for the commission and/or facilitation of a priority offence;
 - d) the level of risk of harm to individuals presented by illegal content of different kinds or by the use of the service for the commission and/or facilitation of a priority offence;
 - e) the level of risk of functionalities of the service facilitating the presence or dissemination of illegal content or the use of the service for the commission or facilitation of a priority offence, identifying and assessing those functionalities that present higher levels of risk;
 - f) the different ways in which the service is used, and the impact of such use on the level of risk of harm that may be suffered by individuals;
 - g) the nature, and severity, of the harm that may be suffered by individuals from the matters identified in accordance with -paragraph (b) to (f) above; and
 - h) how the design and operation of the service (including the business model, governance, use of proactive technology, measures to promote users' media literacy and safe use of the service, and other systems and processes) may reduce or increase the risks identified.
- A2.13 A Provider of a U2U service **must take appropriate steps to keep an illegal content risk assessment up to date**, including when OFCOM makes a significant change to a relevant risk profile.⁷⁹
- A2.14 A Provider of a U2U service is under an obligation **to carry out a further suitable and sufficient illegal content risk assessment, before making any significant changes** to any aspect of a service's design or operation - this further illegal content risk assessment must relate to the impact of that proposed change.⁸⁰

Safety duties about illegal content

- A2.15 Providers of regulated U2U services have specific safety duties in relation to illegal content as set out under Section 10 of the Act. These duties are as follows:
- a) **A duty, in relation to a service, to take or use proportionate measures** relating to the **design or operation of the service** to—
 - i) prevent individuals from encountering priority illegal content by means of the service,
 - ii) effectively mitigate and manage the risk of the service being used for the commission or facilitation of a priority offence, as identified in the most recent illegal content risk assessment of the service, and

⁷⁸ Section 9(5) of the Act.

⁷⁹ Section 9(3) of the Act.

⁸⁰ Section 9(4) of the Act.

- iii) effectively **mitigate and manage the risks of harm to individuals**, as identified in the most recent illegal content risk assessment of the service (see paragraph A2.12(g)).⁸¹
- b) **A duty to operate a service using proportionate systems and processes** designed to—
 - i) minimise the length of time for which any priority illegal content is present;
 - ii) where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way, swiftly take down such content.⁸²
- c) **A duty to include** the following provisions in the **terms of service**:⁸³
 - i) **Provisions specifying how individuals are to be protected from illegal content.** In particular, the terms of service must address how the provider intends to comply with the duty above at paragraph A2.15(b).^{84;85}
 - ii) **Provisions giving information about any proactive technology (see paragraphs A2.81-84 below) used by a service** for the purpose of compliance with the duties set out at paragraphs A2.15(a) or (b) above. This includes setting out the kind of technology that is being used, when it is used, and how it works.⁸⁶
 - iii) Such provisions must be **clear and accessible**.⁸⁷
- d) A duty to **apply the provisions of the terms of service referred to above in paragraph A2.15(c) consistently**.⁸⁸

A2.16 A Provider of a category 1 service will also have **a duty to summarise in the terms of service the findings of the most recent illegal content risk assessment** of a service (including as to levels of risk and as to nature, and severity, of potential harm to individuals).⁸⁹

A2.17 The duties set out at paragraphs A2.15(a) & (b)⁹⁰ apply across all areas of the provider’s U2U service, including the way it is designed, operated and used as well as content present on the service. Among other things, these duties require the provider of a service, if it is proportionate to do so, to take or use measures in the following areas:

- a) regulatory compliance and risk management arrangements,
- b) design of functionalities, algorithms and other features,
- c) policies on terms of use,
- d) policies on user access to the service or to particular content present on the service, including blocking users from accessing the service or particular content,
- e) content moderation, including taking down content,
- f) functionalities allowing users to control the content they encounter,
- g) user support measures, and

⁸¹ Section 10(2)(a)-(c) of the Act.

⁸² Section 10(3)(a)-(b) of the Act.

⁸³ Terms of service is defined under section 237 of the Act as: “in relation to a user-to-user service, means all documents (whatever they are called) comprising the contract for use of the service (or of part of it) by United Kingdom users”.

⁸⁴ Section 10(5) of the Act.

⁸⁵ In relation to paragraph A2.15(b)(i)], the provider must specifically address terrorism content, CSEA content, and other priority illegal content.

⁸⁶ Section 10(7) of the Act.

⁸⁷ Section 10(8) of the Act.

⁸⁸ Section 10(6) of the Act.

⁸⁹ Section 10(9) of the Act.

⁹⁰ Section 10(2)-(3) of the Act.

h) staff policies and practices.⁹¹

A2.18 In determining what is “**proportionate**” for the purposes of the safety duties, the following factors, in particular, are relevant:

- a) all the findings of the most recent illegal content risk assessment, including as to levels of risk and as to nature, and severity, of potential harm to individuals, and
- b) the size and capacity of the provider of a service.⁹²

Duties about content reporting and complaints procedures

A2.19 The duties about content reporting and complaints procedures for providers of U2U services are contained in sections 20 and 21 of the Act.

Duties about content reporting

A2.20 All providers of regulated U2U services are required **to use systems and processes in the operation of their services which allow users and “affected persons” (see 2.23 below) to easily report certain types of content, depending on the kind of service.** For instance, such systems and processes must be put in place to enable users and affected persons to report “illegal content” on *all* U2U services.⁹³

A2.21 For services that are likely to be accessed by children, the duty also applies in respect of content that is harmful to children.^{94,95}

A2.22 Section 8(3)(b) of the Act provides that a duty in relation to a U2U service which is expressed to apply in relation to users of a service extends to the design, operation and use of the service as it affects *United Kingdom* users of the service.

A2.23 For the purposes of the duties about content reporting and complaints procedures (i.e. paragraphs A2.20-26), an “**affected person**” means a person, other than a user of the service in question, who is in the United Kingdom and who is: (a) the subject of the content, (b) a member of a class or group of people with a certain characteristic targeted by the content, (c) a parent of, or other adult with responsibility for, a child who is a user of the service or is the subject of the content, or (d) an adult providing assistance in using the service to another adult who requires such assistance, where that other adult is a user of the service or is the subject of the content.⁹⁶

A2.24 In applying the content reporting duty, the cross-cutting duties will also be relevant.

⁹¹ Section 10(4) of the Act.

⁹² Section 10(10) of the Act.

⁹³ Section 20(2)&(3) of the Act.

⁹⁴ Section 20(2)&(4) of the Act.

⁹⁵ Section 20(6) of the Act states that: “*a provider is only entitled to conclude that it is not possible for children to access a service, or a part of it, if age verification or age estimation is used on the service with the result that children are not normally able to access the service or that part of it.*”

⁹⁶ Section 20(5) of the Act.

Duties about complaints procedures

A2.25 There are two main duties in respect of complaints procedures which apply in relation to all regulated user-to-user services. These are:

- a) **A duty to operate a complaints procedure**, in relation to a service, that:
 - i) allows for relevant kinds of complaint to be made (as set out below),
 - ii) provides for appropriate action to be taken by the provider of the service in response to complaints of a relevant kind, and
 - iii) is easy to access, easy to use (including by children) and transparent.⁹⁷
- b) **A duty to include provisions in the terms of service which are easily accessible (including to children) specifying the policies and processes that govern the handling and resolution of complaints of a relevant kind.**⁹⁸

A2.26 For all services, relevant complaints are:

- a) complaints by users and affected persons about content present on a service which they consider to be illegal content;
- b) complaints by users and affected persons (see definition at paragraph A2.23 if they consider that the provider is not complying with their: Illegal content duties (paragraphs A2.11-18), the content reporting duty (paragraph A2.20), or either of the cross-cutting duties (paragraphs A2.28-34);
- c) complaints by a user who has generated, uploaded or shared content on a service if that content is taken down on the basis that it is illegal content;
- d) complaints by a user of a service if the provider has given a warning to the user, suspended or banned the user from using the service, or in any other way restricted the user's ability to use the service, as a result of content generated, uploaded or shared by the user which the provider considers to be illegal content;
- e) complaints by a user who has generated, uploaded or shared content on a service if—
 - i) the use of proactive technology on the service results in that content being taken down or access to it being restricted, or given a lower priority or otherwise becoming less likely to be encountered by other users, and
 - ii) the user considers that the proactive technology has been used in a way not contemplated by, or in breach of, the terms of service (for example, by affecting content not of a kind specified in the terms of service as a kind of content in relation to which the technology would operate).⁹⁹

A2.27 Services that are likely to be accessed by children and Category 1 services are required to provide for additional types of relevant complaint. For instance, if the service is likely to be accessed by children, then certain complaints regarding the provider's duties in relation to children's online safety will be relevant.¹⁰⁰ For Category 1 services, relevant complaints include complaints that they are not complying with their duties relating to user empowerment, content of democratic importance, news publisher content, journalistic content and freedom of expression and privacy.¹⁰¹

⁹⁷ Section 21(2) of the Act.

⁹⁸ Section 21(3) of the Act.

⁹⁹ Section 21(4)(a)-(e) of the Act.

¹⁰⁰ Section 21(5) of the Act.

¹⁰¹ Section 21(6) of the Act.

Cross-cutting duties

- A2.28 The Act also creates so-called “cross-cutting duties”, which apply to regulated U2U services in relation to the performance of *other* duties under the Act. For instance, the freedom of expression and privacy duties are concerned with how “safety measures and policies” are introduced in relation to a regulated U2U service. These “safety measures and policies” refer to any measures or policies designed to secure compliance with the safety duties in respect of illegal content (section 10, paragraphs A2.15-18), and the duties about content reporting (section 20, paragraphs A2.20-23) and complaints procedures (section 21, paragraphs A2.25-27), as well as other duties in relation to children’s online safety (section 11), and user empowerment (section 15).
- A2.29 In a similar vein, the record-keeping and review duties apply to the performance of the risk assessment duties under section 9 (and section 11); and other “relevant duties”, including the illegal content duties (section 10), and content reporting (section 20) and complaints procedures (section 21).
- A2.30 The cross-cutting duties for regulated U2U services are contained in sections 22 and 23 of the Act.

Duties about freedom of expression and privacy

- A2.31 All regulated U2U services have the following duties when deciding on, and implementing, “safety measures and policies”:
- a) **a duty to have particular regard to the importance of protecting users’ right to freedom of expression within the law,¹⁰² and**
 - b) **a duty to have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a user-to-user service (including, but not limited to, any such provision or rule concerning the processing of personal data).¹⁰³**
- A2.32 In addition, regulated U2U services which are also Category 1 services will have the following duties:
- a) **A duty to carry out impact assessments:**
 - i) when deciding on safety measures and policies, to determine the impact that such measures or policies have on (i) users’ right to freedom of expression within the law, and (ii) the privacy of users;¹⁰⁴ and
 - ii) to determine the impact that any adopted safety measures and policies have on (i) users’ right to freedom of expression within the law, and (ii) the privacy of users.¹⁰⁵

An impact assessment relating to a service must include a section which considers the impact of the safety measures and policies on the availability and treatment on the service of content which is news publisher content or journalistic content in relation to the service.
 - b) **A duty to keep an impact assessment up to date, and to publish impact assessments.¹⁰⁶**

¹⁰² Section 22(2) of the Act.

¹⁰³ Section 22(3) of the Act.

¹⁰⁴ Section 22(4)(a) of the Act.

¹⁰⁵ Section 22(4)(b) of the Act.

¹⁰⁶ Section 22(6) of the Act.

- c) **A duty to specify in a publicly available statement the positive steps that the provider has taken in response to an impact assessment to—** (i) protect users’ right to freedom of expression within the law, and (ii) protect the privacy of users.¹⁰⁷

Record-keeping and review duties

A2.33 All regulated U2U services have the following duties:

- a) **A duty to make and keep a written record**, in an easily understandable form, **of every risk assessment** under section 9 (Illegal Content Risk assessment duties) or 11 (Children’s Risk Assessments).¹⁰⁸
- b) **A duty to make and keep a written record of any measures taken or in use to comply with a relevant duty** which— (a) are described in a Code of Practice and recommended for the purpose of compliance with the duty in question, and (b) apply in relation to the provider and the service in question. Such measures are referred to as “applicable measures in a Code of Practice”.¹⁰⁹
- c) If **alternative measures** (see paragraph A12.33 below) have been taken or are in use to comply with a relevant duty, **a duty to make and keep a written record containing the following information—**
- i) the applicable measures in a Code of Practice that have not been taken or are not in use,
 - ii) the alternative measures that have been taken or are in use,
 - iii) how those alternative measures amount to compliance with the duty in question, and
 - iv) how the provider has had regard to the importance of protecting the right of users to freedom of expression within the law, and protecting the privacy of users in taking or using alternative measures.^{110;111}
- d) **A duty to review compliance with the relevant duties in relation to a service—** (a) regularly, and (b) as soon as reasonably practicable after making any significant change to any aspect of the design or operation of the service.¹¹²

A2.34 ‘Alternative measures’ means measures other than measures which are (in relation to the provider and the service in question) applicable measures in a Code of Practice. If alternative measures have been taken or are in use to comply with the safety duties about illegal content (as at paragraphs A2.15-18 above), or a duty set out in section 11(2) or (3)) of the Act (safety duties protecting children), these records must also indicate whether such measures have been taken or are in use in every area listed at paragraphs A2.17(a)-(h) above or 11(5) (concerning safety duties protecting children), as the case may be, in relation to which there are applicable measures in a Code of Practice (see paragraphs A2.70-85 below).

¹⁰⁷ Section 22(7) of the Act.

¹⁰⁸ Section 23(2) of the Act.

¹⁰⁹ Section 23(3) of the Act.

¹¹⁰ Section 23(4) of the Act.

¹¹¹ Section 49(5) of the Act.

¹¹² Section 23(6) of the Act.

Providers of search services

- A2.35 Providers of regulated search services are also given specific duties under the Act in relation to illegal content. These “Illegal content duties for all search services” include: “Illegal content risk assessment duties”;¹¹³ and “Safety duties about illegal content”.¹¹⁴
- A2.36 Providers of regulated search services are also subject to additional duties which are relevant to illegal content, but also apply to other types of content and in respect of other regulatory requirements as set out under the Act. These are:
- a) “Duties about content reporting and complaints procedures”, which include:
 - i) The “Duty about content reporting”,¹¹⁵ and
 - ii) “Duties about complaints procedures”,¹¹⁶ and
 - b) the “Cross-cutting duties”, which include:
 - iii) “Duties about freedom of expression and privacy”,¹¹⁷ and
 - iv) “Record-keeping and review duties”.¹¹⁸
- A2.37 The Illegal content duties for all search services; Duties about content reporting and complaints procedures; and the Cross-cutting duties that apply to providers of search services are set out in more detail below.
- A2.38 These duties only apply to:
- a) the search content of the service,
 - b) the design, operation and use of the search engine in the United Kingdom, and
 - c) in the case of a duty that is expressed to apply in relation to users of a service, the design, operation and use of the search engine as it affects United Kingdom users of the service.¹¹⁹

Illegal content duties for all search services

Illegal content risk assessment duties

- A2.39 Providers of regulated search services have a duty to carry out a suitable and sufficient illegal content risk assessment¹²⁰ at the times set out in Schedule 3 to the Act.¹²¹

¹¹³ Section 26 of the Act.

¹¹⁴ Section 27 of the Act.

¹¹⁵ Section 31 of the Act.

¹¹⁶ Section 32 of the Act.

¹¹⁷ Section 33 of the Act.

¹¹⁸ Section 34 of the Act.

¹¹⁹ Section 25 of the Act.

¹²⁰ Section 26(2) of the Act.

¹²¹ The deadline for completing the first risk assessment depends on the day on which a search service’s provider starts its operations. In particular:

- i. search services that are already in operation at the outset of this regime must complete their first illegal content risk assessment within a period of three months from the day on which Ofcom’s risk assessment guidance (‘RAG’) is published;

- A2.40 An illegal content risk assessment of a service means an assessment of the following matters, taking into account the risk profile that relates to the service of that kind-
- a) the level of risk of individuals who are users of the service encountering search content of the following kind: (i) each kind of priority illegal content (with each kind separately assessed) and (ii) other illegal content, taking into account (in particular) risks presented by algorithms used by the service, and the way that the service indexes, organises, and presents search results;
 - b) the level of risk of functionalities of the service facilitating individuals encountering search content that is illegal content, identifying and assessing those functionalities that present higher levels of risks;
 - c) the nature, and severity, of the harm that might be suffered by individuals from the matters identified in accordance with paragraphs (a) and (b) above; and;
 - d) how the design and operation of the service (including the business model, governance, use of proactive technology, measures to promote users' media literacy and safe use of the service, and other systems and processes) may reduce or increase the risks identified.¹²²
- A2.41 After completing the first illegal content risk assessment, providers of regulated search services are under **a duty to take appropriate steps to keep an illegal content risk assessment up to date**, including when Ofcom make any significant change to a risk profile that relates to the services of the kind in question.¹²³
- A2.42 Before making any significant change to any aspect of a service's design or operation, providers of regulated search services are under a duty to carry out a further suitable and sufficient illegal content risk assessment relating to the impacts of the proposed change¹²⁴.

Safety duties about illegal content

- A2.43 Providers of regulated search services have specific Safety duties in relation to illegal content as set out under section 27 of the Act. These duties are as follows:
- a) **A duty**, in relation to a service, **to take or use proportionate measures relating to the design or operation of the service to effectively mitigate and manage the risks of harm to individuals, as identified in the most recent illegal content risk assessment of the service** (see paragraphs A2.39-42 above).¹²⁵
 - b) **A duty to operate a service using proportionate systems and processes designed to minimise the risk of individuals encountering search content** of the following kinds—
 - i) **priority illegal content**; and

-
- ii. new search services that start operations after the RAG is published must complete their first illegal content risk assessment within a period of three months from the day on which they begin their new services; and
 - iii. existing services that become search services (having previously provided a different type of service) after the RAG is published must complete their first illegal content risk assessment within a period of three months from the day on which their service becomes a search service.

See Schedule 3 to the Act.

¹²² Sections 26(5)(a)-(d) of the Act.

¹²³ Section 26(3) of the Act.

¹²⁴ Section 26(4) of the Act.

¹²⁵ Section 27(2) of the Act.

- ii) **other illegal content** that the provider knows about (having been alerted to it by another person or become aware of it in any other way).¹²⁶
- c) **A duty to include provisions in a publicly available statement specifying how individuals are to be protected from search content that is illegal content.**¹²⁷
- d) **A duty to apply the provisions of the statement referred to at paragraph A2.43(c) above consistently.**¹²⁸
- e) **A duty to include provisions in a publicly available statement giving information about any proactive technology** (see paragraphs A2.81-84 below) used by a service for the purpose of compliance with a duty set out in sections 27(2) or (3) (paragraphs A2.43(a) or (b) above) (including the kind of technology, when it is used, and how it works).¹²⁹
- f) **A duty to ensure that the provisions of the publicly available statement** referred to in sections 27(5) and (7) (paragraphs A12.43(c)&(e) above) are **clear and accessible.**¹³⁰

A2.44 The duties set out in paragraphs A2.43(a)-(b) above apply across all areas of a service, including the way the search engine is designed, operated and used as well as search content of the service. Among other things, these duties require the provider of a service to take or use measures in the following areas, if it is proportionate to do so:

- a) regulatory compliance and risk management arrangements,
- b) design of functionalities, algorithms and other features relating to the search engine,
- c) functionalities allowing users to control the content they encounter in search results,
- d) content prioritisation,
- e) user support measures, and
- f) staff policies and practices.¹³¹

A2.45 In determining what is ‘**proportionate**’ for the purposes of the safety duties for search services, the following factors, in particular, are relevant:

- a) all the findings of the most recent illegal content risk assessment (including as to levels of risk and as to nature, and severity, of potential harm to individuals), and
- b) the size and capacity of the provider of a service.¹³²

Duties about content reporting and complaints procedures

Duty about content reporting

A2.46 All providers of regulated search services are required **to operate a service using systems and processes that allow users and ‘affected persons’ to easily report certain types of search content, depending on the type of service.**¹³³ For instance, such systems and processes must be put in place to enable users and affected persons to report ‘illegal content’ on *all* of the search service.¹³⁴

¹²⁶ Section 27(3) of the Act.

¹²⁷ Section 27(5) of the Act.

¹²⁸ Section 27(6) of the Act.

¹²⁹ Section 27(7) of the Act.

¹³⁰ Section 27(8) of the Act.

¹³¹ Section 27(4) of the Act.

¹³² Section 27(10) of the Act.

¹³³ Section 31(2) of the Act.

¹³⁴ Section 31(3) of the Act.

- A2.47 For services that are likely to be accessed by children, the duty also applies in respect of content that is harmful to children.¹³⁵
- A2.48 Section 25(1)(c) of the Act provides that a duty in relation to a search service which is expressed to apply in relation to users of a service extends to the design, operation and use of the search engine as it affects *United Kingdom* users of the service.
- A2.49 For the purposes of the duties about content reporting and complaints procedures (i.e. paragraphs A2.46-52), an “affected person” has the same definition as for U2U services (see paragraphs A2.23 above).

Duties about complaints procedures

A2.50 There are two main duties in respect of complaints procedures which apply in relation to all regulated search services. These are as follows:

- a) **A duty to operate a complaints procedure** in relation to a service that—
- i) allows for relevant kinds of complaint to be made (as set out below),
 - ii) provides for appropriate action to be taken by the provider of the service in response to complaints of a relevant kind, and
 - iii) is easy to access, easy to use (including by children) and transparent.¹³⁶
- b) **A duty to make the policies and processes that govern the handling and resolution of complaints of a relevant kind publicly available and easily accessible (including to children).**¹³⁷

A2.51 Relevant complaints in relation to a regulated search service are:

- a) complaints by users and affected persons (see paragraph A2.23 above) about search content which they consider to be illegal content;
- b) complaints by users and affected persons if they consider that the provider is not complying with their illegal content duties (paragraph A2.39-45), content reporting duties (paragraphs A2.46-49), or freedom of expression and privacy (see paragraph A2.57);
- c) complaints by an interested person if the provider of a search service takes or uses measures in order to comply with their safety duties (paragraphs A2.43-45) that result in content relating to that interested person no longer appearing in search results or being given a lower priority in search results;
- d) complaints by an interested person if—
 - i) the use of proactive technology (see paragraphs A2.81-84 below) on a search service results in content relating to that interested person no longer appearing in search results or being given a lower priority in search results; and
 - ii) the interested person considers that the proactive technology has been used in a way not contemplated by, or in breach of, the provider’s policies on its use (for example, by affecting content not of a kind specified in those policies as a kind of content in relation to which the technology would operate).¹³⁸

A2.52 A complaint may also be a relevant complaint in the specific context of the service that is being provided. For instance, if the service is likely to be accessed by children, then certain

¹³⁵ Section 31(4) of the Act.

¹³⁶ Section 32(2)(a)-(c) of the Act.

¹³⁷ Section 32(3) of the Act.

¹³⁸ Section 32(4)(a)-(d) of the Act.

complaints regarding the provider’s duties in relation to children’s online safety will be relevant.¹³⁹

- A2.53 For the purposes of the duties about complaints procedures for regulated search services, an ‘interested person’ means a person that is responsible for a website or database capable of being searched by the search engine, provided that—
- a) in the case of an individual, the individual is in the United Kingdom;
 - b) in the case of an entity, the entity is incorporated or formed under the law of any part of the United Kingdom.¹⁴⁰

Cross-cutting duties

- A2.54 The Act also creates ‘cross-cutting’ duties which apply to regulated search services in relation to the performance of other duties under the Act. For instance, the duties about freedom of expression and privacy are concerned with how “safety measures and policies” are introduced in relation to a regulated search service. These “safety measures and policies” refer to any measures or policies designed to secure compliance with the safety duties about illegal content (section 27, paragraphs A2.43-5 above), and the duty about content reporting (section 31, paragraphs A2.46-49 above), and duties about complaints procedures (section 32, paragraphs A2.50-53 above), as well as other duties in relation to children’s online safety (section 29 – these duties are beyond the scope of this consultation).
- A2.55 In a similar vein, the record-keeping and review duties apply to the performance of the risk assessment duties under section 26 (paragraph A2.39-42) and section 28 (Children’s risk assessment duties); and other “relevant (duties)”, including the safety duties in respect of illegal content (paragraphs A2.43-45 above), and content reporting and complaints procedures (see sections 31 and 32, paragraphs A2.46-53).
- A2.56 The cross-cutting duties for regulated search services are set out in sections 33 and 34 of the Act.

Duties about freedom of expression and privacy

- A2.57 All regulated search services have the following duties when deciding on, and implementing, “safety measures and policies” (see above):
- a) **a duty to have particular regard to the importance of protecting the rights of users and interested persons to freedom of expression within the law;**¹⁴¹ and
 - b) **a duty to have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy** that is relevant to the use or operation of a search service (including, but not limited to, any such provision or rule concerning the processing of personal data).¹⁴²

Record-keeping and review duties

- A2.58 All regulated search services have the following duties:

¹³⁹ Section 32(5)(a)-(d) of the Act.

¹⁴⁰ Section 32(6) & 228(7) of the Act.

¹⁴¹ Section 33(2) of the Act.

¹⁴² Section 33(3) of the Act.

- a) **A duty to make and keep a written record, in an easily understandable form, of every risk assessment** made under section 26 (see paragraphs A2.39-42] above) or 28 (children’s risk assessment duties).¹⁴³
- b) **A duty to make and keep a written record of any measures taken or in use** to comply with a relevant duty (see paragraph A2.55 above) which—
 - i) are described in a Code of Practice and recommended for the purpose of compliance with the duty in question, and
 - ii) apply in relation to the provider and the service in question. In this section such measures are referred to as “applicable measures in a code of practice”.¹⁴⁴
- c) If alternative measures have been taken or are in use to comply with a relevant duty, **a duty to make and keep a written record containing the following information—**
 - iii) the applicable measures in a Code of Practice that have not been taken or are not in use,
 - iv) the alternative measures that have been taken or are in use,
 - v) how those alternative measures amount to compliance with the duty in question, and
 - vi) how the provider has had regard to the importance of protecting the right of users and interested persons to freedom of expression within the law, and protecting the privacy of users in taking or using alternative measures (i.e. under section 49(5)).¹⁴⁵

If alternative measures have been taken or are in use to comply with the safety duties about illegal content (specifically sections 27(2) or (3), as at paragraphs 42(a)-(b) above), or a duty set out in section 29(2) or (3) of the Act (Safety duties protecting children), this record must also indicate whether such measures have been taken or are in use in every area listed at paragraphs A2.43(a)-(f) above or section 29(4) (concerning Safety duties protecting children) (as the case may be) in relation to which there are applicable measures in a Code of Practice (see paragraphs A2.70-85).¹⁴⁶
- d) **A duty to review compliance with the relevant duties in relation to a service—** regularly, and as soon as reasonably practicable after making any significant change to any aspect of the design or operation of the service.¹⁴⁷

A2.59 Ofcom may provide that particular descriptions of providers of search services are exempt from any or all of the record-keeping and review duties, and must publish details of any exemption.¹⁴⁸

Ofcom’s duties in relation to illegal content

A2.60 The Act gives specific duties to Ofcom in relation to illegal content. These are set out below.

¹⁴³ Section 34(2) of the Act.

¹⁴⁴ Section 34(3) of the Act.

¹⁴⁵ Section 34(4)(a)-(d) of the Act.

¹⁴⁶ Section 34(5) of the Act.

¹⁴⁷ Sections 34(6)(a)&(b) of the Act.

¹⁴⁸ Section 34(7) of the Act.

Ofcom sector risk assessment

- A2.61 Ofcom is under a duty to carry out a risk assessment to identify and assess the risks of harm to individuals in the UK caused by:
- a) illegal content on U2U services and by the use of U2U services for the commission and/or facilitation of priority offences (the “illegality risks”);
 - b) illegal content that appears to individuals in search results encountered on search services (“risk of harm from illegal content” and, together with the “illegality risks”, the “risks of harm”).¹⁴⁹
- A2.62 It has a discretion whether to combine these or consider them separately (also with the risk of harm to children under section 98(1)(c)).¹⁵⁰
- A2.63 Ofcom’s risk assessment must, among other things, identify the characteristics of U2U and search services (which include functionalities, user base, business model and governance, and other systems and processes) that are relevant to the risks of harm and assess the impact of these characteristics on the risks of harm.¹⁵¹

Register of Risks and Risk Profiles

- A2.64 Ofcom must prepare and publish a register of risks that reflects the findings of its risk assessments (the ‘Register of Risks’). The Register of Risks must be prepared as soon as reasonably practicable after completion of the risk assessments.¹⁵²
- A2.65 Further to the Register of Risks, after completing its risk assessments, Ofcom must prepare and publish Risk Profiles for U2U services and search services that relate to each risk of harm, as applicable (the ‘Risk Profiles’). In preparing the Risk Profiles, Ofcom can group U2U services and search services as appropriate and having regard to (i) the characteristics of the services and (ii) the risk levels and other matters identified in the risk assessment.¹⁵³
- A2.66 Ofcom must review and revise the risk assessments and the Risk Profiles from time to time to keep them up to date.¹⁵⁴

Risk assessment guidance for services

- A2.67 Ofcom must prepare and publish guidance to help U2U services and search services comply with their duties to prepare illegal content risk assessments under sections 9 and 26 respectively (the ‘Risk Assessment Guidance’ or ‘RAG’) (please refer to paragraphs A2.60-67).¹⁵⁵
- A2.68 Ofcom must prepare the RAG as soon as reasonably practicable after having published the risk profiles relating to the risks of harm.
- A2.69 Ofcom must revise and publish an updated RAG when it carries out a new risk assessment and/or revises the risk profiles.¹⁵⁶

¹⁴⁹ Sections 98(1)(a)&(b) of the Act.

¹⁵⁰ Sections 98(3) of the Act.

¹⁵¹ Sections 98(2)&(11) of the Act.

¹⁵² Section 98(4) of the Act.

¹⁵³ Section 98(5)-(7) of the Act.

¹⁵⁴ Section 98(8) of the Act.

¹⁵⁵ Sections 99(1)&(2) of the Act.

¹⁵⁶ Sections 99(5) of the Act.

“Illegal” Codes for U2U and search

Ofcom’s duty to prepare and issue Codes of Practice in relation to illegal content

A2.70 Ofcom must prepare and issue Codes of Practice for providers of regulated U2U services and providers of regulated search services. The Codes of Practice must describe the measures Ofcom recommends these providers take for the purposes of complying with:

- a) their respective safety duties in respect of illegal content (see sections 10 and 27, paragraphs A2.15-18 and 2.43-45), so far as they relate to:
 - i) Terrorism content or offences, as set out in Schedule 5 of the Act;¹⁵⁷ and
 - ii) CSEA content or offences, as set out in Schedule 6 of the Act;¹⁵⁸ and
- b) the relevant duties (except to the extent they overlap with paragraphs A2.70(a)(i) and (ii) above).¹⁵⁹ These include: the safety duties in respect of illegal content (see paragraphs A2.15-18 and 2.43-45); content reporting duties (see paragraphs A2.20-23 and A2.46-58); and complaints procedure duties (see paragraphs A2.22-27, and A2.50-53).¹⁶⁰

A2.71 Schedule 4 of the Act sets out general principles and online safety objectives which the Codes must follow, as well as what content must be included. These are set out below.

General principles

A2.72 In preparing a draft Code, Ofcom must consider the appropriateness of provisions of the Code to different kinds and sizes of U2U and search services, and to providers of differing sizes and capacities (paragraph 1 of Schedule 4). It must also have regard to the following principles:

- a) providers of U2U and search services must be able to understand which provisions of the Code of Practice apply in relation to a particular service they provide;
- b) the measures described in the Code of Practice must be sufficiently clear, and at a sufficiently detailed level, that providers understand what those measures entail in practice;
- c) the measures described in the Code of Practice must be proportionate and technically feasible: measures that are proportionate or technically feasible for providers of a certain size or capacity, or for services of a certain kind or size, may not be proportionate or technically feasible for providers of a different size or capacity or for services of a different kind or size;
- d) the measures described in the Code of Practice that apply in relation to U2U and search service providers of various kinds and sizes must be proportionate to Ofcom’s assessment of the risk of harm presented by services of that kind or size (see paragraphs A2.57-59 above).¹⁶¹

¹⁵⁷ Section 41(1) of the Act.

¹⁵⁸ Section 41(2) of the Act.

¹⁵⁹ Section 41(3) of the Act.

¹⁶⁰ Section 41(10) of the Act.

¹⁶¹ Schedule 4 of the Act, subparagraphs 2(a)-(d).

Online safety objectives

A2.73 Ofcom must ensure that any measures described in the Codes are compatible with the pursuit of the online safety objectives.¹⁶²

A2.74 For **U2U services**, these are:

- a) That a service should be designed and operated in such a way that—
 - i) the systems and processes for regulatory compliance and risk management are effective and proportionate to the kind and size of service;
 - ii) the systems and processes are appropriate to deal with the number of users of the service and its user base;
 - iii) UK users (including children) are made aware of, and can understand, the terms of service;
 - iv) there are adequate systems and processes to support United Kingdom users;
 - v) (in the case of a Category 1 service) users are offered options to increase their control over the content they encounter and the users they interact with;
 - vi) the service provides a higher standard of protection for children than for adults;
 - vii) the different needs of children at different ages are taken into account;
 - viii) there are adequate controls over access to the service by adults;
 - ix) there are adequate controls over access to, and use of, the service by children, taking into account use of the service by, and impact on, children in different age groups; and
- b) that a service should be designed and operated so as to protect individual UK users from harm, including with regard to—
 - i. algorithms used by the service,
 - ii. functionalities of the service, and
 - iii. other features relating to the operation of the service.¹⁶³

A2.75 For **search services**, these are:

- a) That a service should be designed and operated in such a way that—
 - i) the systems and processes for regulatory compliance and risk management are effective and proportionate to the kind and size of service;
 - ii) the systems and processes are appropriate to deal with the number of users of the service and its user base;
 - iii) United Kingdom users (including children) are made aware of, and can understand, the publicly available statement referred to in relation to the safety duties (paragraph A2.43(c) above) and the safety duties protecting children (section 29);
 - iv) there are adequate systems and processes to support United Kingdom users;
 - v) the service provides a higher standard of protection for children than for adults;
 - vi) the different needs of children at different ages are taken into account; and
- b) that a service should be assessed to understand its use by, and impact on, children in different age groups; and
- c) that a search engine should be designed and operated so as to protect individuals in the United Kingdom who are users of the service from harm, including with regard to—

¹⁶² Schedule 4 of the Act, paragraph 3.

¹⁶³ Schedule 4 of the Act, subparagraphs 4(a)-(b).

- i. algorithms used by the search engine,
- ii. functionalities relating to searches (such as a predictive search functionality), and
- iii. the indexing, organisation and presentation of search results.¹⁶⁴

A2.76 For **combined services**, these are:

- a) That the online safety objectives that apply to U2U services (paragraphs A2.70 (a)-(b) above) do not apply in relation to the search engine;
- b) That the online safety objectives that apply to search services apply in relation to the search engine (and, accordingly, in this context, references to a search service include the search engine);
- c) That the reference in a publicly available statement (as at paragraph A2.43(c) above) includes a reference to provisions of the terms of service which relate to the search engine.¹⁶⁵

A2.77 The Secretary of State may amend these objectives by way of regulations.¹⁶⁶

Content of Codes of Practice

A2.78 The Act also sets out what type of measures must be included in the content of the Codes, and the principles in relation to which such measures should be designed. Such measures may only relate to the design or operation of the relevant service in the United Kingdom, or as it affects United Kingdom users of the service. In particular:

- a) The Codes of Practice describing measures recommended for the purpose of compliance with the safety duties for providers of U2U services set out at paragraphs A2.18(a)&(b) above (i.e. in relation to taking proportionate measures relating to the design or operation of the service, or to operate a service using proportionate systems and processes), must include measures in each of the areas of a service listed at paragraphs A2.17(a)-(h), to the extent that inclusion of the measures in question is consistent with:
 - i) their appropriateness to different kinds and sizes of services and to providers of differing sizes and capacities;
 - ii) the principle that measures should be proportionate and technically feasible; measures that are proportionate or technically feasible for providers of a certain size or capacity, or for services of a certain kind or size, may not be proportionate or technically feasible for providers of a different size or capacity or for services of a different kind or size;
 - iii) the principle that the measures described in the code of practice that apply in relation to services of various kinds and sizes must be proportionate to OFCOM's assessment (under section 98) of the risk of harm presented by services of that kind or size.¹⁶⁷
- b) Codes of practice that describe measures recommended for the purpose of compliance with the Safety Duties about illegal content for providers of search services set out at paragraphs A12.42(a)&(b) (i.e. in relation to taking proportionate measures relating to the design or operation of the service, or to operate a service using proportionate

¹⁶⁴, subparagraphs (5)(a)-(c).

¹⁶⁵ Schedule 4 of the Act, subparagraphs 6(a)-(c).

¹⁶⁶ Schedule 4 of the Act, paragraph 7.

¹⁶⁷ Schedule 4 of the Act, subparagraphs 9(1) and 9(5).

systems and processes) must include measures in each of the areas of a service listed at paragraphs A2.43(a)-(f) above, to the extent that inclusion of the measures in question is consistent with paragraph A2.78(a)i) to iii) above.^{168 169}

A2.79 Any measures described in a Code of Practice which are recommended for the purpose of compliance with any of the relevant duties must be designed in the light of the following principles:

- a) the importance of protecting the right of users and (in the case of search services or combined services) interested persons to freedom of expression within the law, and
- b) the importance of protecting the privacy of users.¹⁷⁰

A2.80 Where appropriate, such measures must also incorporate safeguards for the protection of the matters mentioned in those principles.

Proactive technology

A2.81 If Ofcom considers it appropriate to do so, and in accordance with the general principles set out at paragraphs 1 and 2 of Schedule 4 (see paragraphs A12.72-76) and the principles set out at paragraph 10(2) of Schedule 4 (see paragraph A2.79), it may include in a Code of Practice a measure describing the use of a kind of technology. However, there are constraints on Ofcom's power to include a measure describing the use of "proactive technology" (a "proactive technology measure"). Section 231 defines "proactive technology" as consisting of three types of technology: content identification technology, user profiling technology, and behaviour identification technology (subject to certain exceptions). These are explained in greater detail below.

A2.82 Content identification technology refers to technology, such as algorithms, keyword matching, image matching or image classification, which analyses content to assess whether it is content of a particular kind (for example, illegal content). Content identification technology is not regarded as proactive technology if it is used in response to a report from a user or other person about particular content.

A2.83 User profiling technology means technology which analyses (any or all of) relevant content (as defined in section 231(8)), user data, or metadata relating to relevant content or user data, for the purposes of building a profile of a user to assess characteristics such as age. However, technology which analyses data specifically provided by a user for the purposes of the provider verifying or estimating the user's age in order to decide whether to allow the user to access a service (or part of a service) or particular content, but which does not analyse any other data or content, is not regarded as user profiling technology.

A2.84 Behaviour identification technology means technology which analyses (any or all of) relevant content (as defined in section 231(8)), user data, or metadata relating to relevant content or user data, to assess a user's online behaviour or patterns of online behaviour (for example, to assess whether a user may be involved in, or be the victim of, illegal activity). But behaviour identification technology is not regarded as proactive technology if it is used in response to concerns identified by another person or an automated tool about a particular user.

¹⁶⁸ The measures set out in Section 27(4) of the Act.

¹⁶⁹ Schedule 4 of the Act, subparagraphs 9(3) and 9(5).

¹⁷⁰ This refers to protecting the privacy of users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a U2U or search service (including any provisions concerning the processing of personal data), Schedule 4 of the Act, paragraph 10(4).

A2.85 Ofcom has power to include a proactive technology measure in a Code of Practice for the purpose of compliance with the safety duties in relation to illegal content set out in sections 10(2) or (3) (for U2U services), or in sections 27(2) or (3) (for search services).¹⁷¹ However, that power is subject to the following constraints:

- a) A proactive technology measure may not recommend the use of technology which operates (or may operate) by analysing user-generated content communicated privately, or metadata relating to such content.¹⁷²
- b) A proactive technology measure may be included in a Code of Practice in relation to services of a particular kind or size only if Ofcom is satisfied that the use of the technology by such services would be proportionate to the risk of harm that the measure is designed to safeguard against (taking into account, in particular, Ofcom's risk profile relating to such services published under section 98, see paragraphs A2.64-66).¹⁷³
- c) In deciding whether to include a proactive technology measure in a Code of Practice, Ofcom must have regard to the degree of accuracy, effectiveness and lack of bias achieved by the technology in question. Ofcom may also refer in the Code of Practice to existing industry or technical standards for the technology (where they exist), or set out principles in the Code of Practice designed to ensure that the technology or its use is (so far as possible) accurate, effective and free of bias.¹⁷⁴

Relationship between provider duties and Ofcom's Codes of Practice

A2.86 Providers of a regulated U2U or search service who take or use the measures described in a Code of Practice which are recommended for the purpose of complying with a relevant duty will be treated as having complied with that relevant duty.¹⁷⁵ Further, providers who take or use the relevant recommended measures that incorporate safeguards to protect users' rights to freedom of expression within the law, and to protect the privacy of users, respectively, will be treated as having complied with the freedom of expression and privacy duties set out in sections 22(2)-(3), for U2U services, and sections 33(2)-(3), for search services, respectively.¹⁷⁶

A2.87 Where a provider adopts an alternative measure to those described in a Code of Practice in order to comply with a relevant duty, it must have particular regard to the importance of: protecting the right of users and (in the case of search services) interested persons to freedom of expression within the law, and protecting the privacy of users.¹⁷⁷

A2.88 When it is assessing whether a provider of a service is compliant with a relevant duty where that provider has adopted an alternative measure, Ofcom must consider the extent to which an alternative measure taken or in use by the provider extends across the relevant duties (i.e. under sections 10(4), or 29(4)), and, where appropriate, that it incorporates safeguards

¹⁷¹ Paragraph 13(3) of Schedule 4 of the Act sets out that a proactive technology measure may also be recommended for the purpose of compliance with the children's online safety duties set out in section 12(2) or (3) of the Act (in relation to U2U services) or section 29(2) or (3) of the Act (in relation to search services), or for the purpose of compliance with the fraudulent advertising duties set out in section 38(1) or 39(1) of the Act.

¹⁷² See paragraph 13(4) of Schedule 4 of the Act. For factors which Ofcom must particularly consider when deciding whether content is communicated "publicly" or "privately" by means of a user-to-user service for these purposes, see section 232.

¹⁷³ See paragraph 13(5) of Schedule 4 of the Act.

¹⁷⁴ See paragraph 13(6) of Schedule 4 of the Act. This requirement does not apply to proactive technology which is a kind of age verification or age estimation technology: see paragraph 13(7) of Schedule 4 of the Act.

¹⁷⁵ Section 49(1) of the Act.

¹⁷⁶ Section 49(2)-(3) of the Act.

¹⁷⁷ Section 49(5) of the Act.

for the protection of the right of users and (in the case of search services) interested persons to freedom of expression within the law, and protection of the privacy of users.¹⁷⁸

Effect of the Codes of Practice

A2.89 Failure to comply with a provision of a Code of Practice does not in itself make the provider liable to legal proceedings in a court or tribunal,¹⁷⁹ although the Code will be admissible in evidence in legal proceedings,¹⁸⁰ and any such court or tribunal must take a provision of the Code into account when determining a question which is relevant to that provision, as long as the question relates to a time when the provision was in force.¹⁸¹ Similarly, Ofcom must take into account a provision of a Code of Practice when determining a question which is relevant to that provision, as long as the question relates to a time when the provision was in force.¹⁸²

Illegal Content Judgements Guidance

A2.90 Providers of regulated U2U or search services complying with their duties as set out above will need to make judgments about whether content is content of a particular kind, on the basis of all relevant information reasonably available to them.¹⁸³ This includes decisions in relation to whether a provider has reasonable grounds to infer that content is content is illegal content, or illegal content of a particular kind.¹⁸⁴

A2.91 In order to make a judgement that content is illegal content, providers will need reasonable grounds to infer that all of the elements necessary for the commission of the offence, including the mental elements, are present or satisfied,¹⁸⁵ and that no defence to the offence may be successfully relied upon.¹⁸⁶

A2.92 To assist providers in making these judgments in relation to illegal content, Ofcom must produce and publish Illegal Content Judgments Guidance ('ICJG').¹⁸⁷

Enforcement guidance

A2.93 Ofcom must produce guidance for providers of regulated services about how it proposes to exercise its functions in relation to enforcement (these functions are set out at sections 130-150).¹⁸⁸ This guidance must give information about the factors Ofcom would consider it appropriate to take into account when taking, or considering taking, enforcement action relating to a provider's failure to comply with the different "enforceable requirements" set out in section 131 of the Act.¹⁸⁹ These include all of the duties set out above at paragraphs A2.5 – 59 above. The Guidance must also include provision explaining how Ofcom will take into account the impact or possible impact of such a failure on children when considering a failure to comply with the illegal content duties (sections 10 or 27), or any of the duties relating to children's online safety (sections 12 or 29) or children's access to provider

¹⁷⁸ Section 49(6) of the Act.

¹⁷⁹ Section 50(1) of the Act.

¹⁸⁰ Section 50(2) of the Act.

¹⁸¹ Section 50(3) of the Act

¹⁸² Section 50(4) of the Act.

¹⁸³ Section 192 of the Act.

¹⁸⁴ Sections 192(4)&(5) of the Act.

¹⁸⁵ Section 192(6)(a) of the Act.

¹⁸⁶ Section 192(6)(b) of the Act.

¹⁸⁷ Section 193 of the Act.

¹⁸⁸ Section 151(1) of the Act.

¹⁸⁹ Section 151(2) of the Act.

pornographic content (section 81(2)).¹⁹⁰ Ofcom must have regard to this guidance when exercising their functions in relation to enforcement, or deciding whether to exercise them.¹⁹¹

Record keeping guidance

A2.94 Ofcom must produce guidance for providers of regulated U2U and search services to assist them in complying with their record-keeping and review duties (sections 23 (U2U) and 34 (search)) – paragraphs A2.33-34, and A2.58-59 above.¹⁹²

Penalty guidelines

A2.95 Ofcom must prepare and publish a statement containing the guidelines they propose to follow in determining the amount of penalties imposed by them.¹⁹³

¹⁹⁰ Section 151(3) of the Act.

¹⁹¹ Section 151(7) of the Act.

¹⁹² Section 52(3) of the Act.

¹⁹³ Section 392(1) of the Communications Act 2004. See also Schedule 13 of the Act, sub-paragraph 2(5).