Online Safety Information Powers Guidance

Draft updated guidance for information gathering powers under the Online Safety Act 2023

Consultation

Published: 16 September 2025
Closing date for responses: 28 October 2025

Contents

Section

1. Overview

1.1 Ofcom is the independent regulator for online safety in the UK. The statutory information gathering powers conferred on Ofcom by the Online Safety Act 2023 (the 'Act') give us the legal tools to obtain information in support of our online safety functions.

1.2 This Online Safety Information Powers Guidance (the 'Guidance') is intended to help regulated services and other stakeholders understand what our online safety information gathering powers are, when and how we might use each power, the obligations on stakeholders to comply with the powers and the potential consequences of non-compliance. The Guidance is non-binding, setting out what we will generally do, but we will always consider the use of powers on a case-by-case basis and may sometimes depart from the approach set out in the Guidance. Where we do so, we will explain our reasons for doing so.

2. Introduction

2.1 The information gathering powers conferred on Ofcom by the Act give us the legal tools to obtain information for the purpose of exercising, or deciding whether to exercise, any of our online safety functions.

2.2 The aim of this Guidance is to help stakeholders to understand what Ofcom's online safety information gathering powers are, when and how we might use each power, the duties on services and other people to comply and the potential consequences of non-compliance.

2.3 This document is split into the following section as shown in Table 2.1 below.

Table 2.1: Information gathering powers in the Act and where to find them in this document

Section in the Guidance	Section/ Schedule in the Act	What the section covers (relevant powers)	Location in the Guidance (paragraph)
Section 2	N/A	Introduction, covering the scope and status of this Guidance	2.1 – 2.12
Section 3	N/A	Ofcom's general approach to information gathering, including how we typically decide how to use our powers, how we will treat confidential information, how we will handle personal data and how we will disclose information	3.1 – 3.66
Section 4	s100 - s103	The power to issue information notices, including:	4.1 – 4.97
		• specific considerations for section 100 notices requiring the performance of a test	4.37 – 4.50
		• specific considerations for section 100 notices requiring the remote viewing of certain information under section 100(3) ('Remote Viewing Information Notice')	4.51 – 4.71
		• specific considerations for section 101(C1) notices requiring the retention of information relating to the use of a service by a child who has died ('Data Preservation Notices'[1])	4.72-4.87
		• specific considerations for section 101(1) notices requiring the provision of information relating to the use of a service by a child who has died ('Coroner Information Notice')	4.88 – 4.104
		• requirement to name a senior manager under section 103	4.105- 4.114
Section 5	s104	Skilled persons' reports	5.1 – 5.18

[1] Ofcom's functions in relation to Data Preservation Notices are triggered when Ofcom receives a notification from a coroner (in England, Wales and Northern Ireland) or a Procurator Fiscal (in Scotland). For convenience, we refer only to coroners in this document, but references to coroners include references to Procurators Fiscal in Scotland.

Section in the Guidance	Section/ Schedule in the Act	What the section covers (relevant powers)	Location in the Guidance (paragraph)
Section 6	s106	Interviews	6.1 – 6.19
Section 7	Sch12	Entry, inspection and audit	7.1 – 7.44
Section 8	N/A	The duties imposed on services and other persons and the consequences of non-compliance with any of these information gathering powers	8.1 – 8.12

The scope of this Guidance

2.4 This Guidance covers Ofcom's information gathering powers as set out in Part 7, Chapter 4 of and Schedule 12 to the Act. Table 2.1 lists these powers, with references to the appropriate sections of this document.

2.5 Ofcom also exercises information gathering powers set out in other legislation relating to the areas that we regulate, including the Communications Act 2003, the Wireless Telegraphy Act 2006, and the Postal Services Act 2011. This guidance does not cover the exercise of those powers. We have a general information gathering policy that applies to those powers.[2]

2.6 Ofcom may also gather information from sources using methods other than a statutory information gathering power, such as:

a) public sources, for instance published research or openly available material on services' websites;
b) data purchased from third party intelligence services;
c) information provided informally by services, for example in the course of supervisory discussions;
d) data from complaints submitted by members of the public; and
e) information provided to us by other bodies, such as other regulators,[3] MPs, consumer organisations or entities eligible to make super complaints under the Act.

2.7 These other sources and methods of information gathering are not covered in this Guidance.[4]

The status of this Guidance

2.8 The Act does not require us to produce guidance on how we are likely to exercise our information gathering powers, but we have decided to do so to assist stakeholders.

2.9 This Guidance provides an overview of Ofcom's information gathering powers under the Act, how we will generally exercise our information gathering powers and the processes we will typically follow. The Guidance is indicative only and is designed to be

[2] General Policy on Information Gathering 2024.
[3] This may include, but is not limited to, other members of the Digital Regulation Cooperation Forum (CMA, FCA and ICO).
[4] Paragraph 3.5 of our Online Safety Enforcement Guidance provides examples of sources of information Ofcom may receive information used to identify and assess potential compliance issues.

flexible – we will always consider the use of our information powers on a case-by-case basis, which means we may sometimes depart from the processes described in this document. Where we do depart from this Guidance, we will explain the reasons why. Examples may include, but are not limited to, when we must act in a particular way by a court or tribunal or as part of a sensitive investigation.

2.10 The Guidance is not a substitute for any regulation or law and is not legal advice. We will keep this Guidance under review and amend it as appropriate in light of further experience, developing law and practice and any change to Ofcom's functions.

Persons in scope of our information gathering powers

2.11 The persons from whom we may gather information differ depending on which of our information gathering powers we are exercising. For example, we can issue an information notice under section 100(1) of the Act to a wide range of people, including any person who appears to us to have, or to be able to generate or obtain, information that we require. In contrast, we can only issue a Coroner Information Notice under section 101(1) to a provider of a regulated service, a provider of an ancillary service or access facility, or a person who was a provider of such a service at a time to which the required information relates.

2.12 Table 2.2 provides an overview of the persons from whom we may gather information under each information gathering power.

Table 2.2: Persons who may be legally bound by Ofcom's information gathering powers

Power	(i) Provider of regulated service	(ii) Provider of ancillary service or access facility	(iii) A person who was within (i) or (ii) at a time to which the information relates	(iv) Any other person	(v) Certain individuals connected to regulated services
Section 100 – information notice	X	X	X	X	
Section 100(3) – Remote Viewing Information Notice	X	X			
Section 101(C1) – Data Preservation Notice	X	X	X		
Section 101(1) – Coroner Information Notice	X	X	X		
Section 103 – requirement to name a senior manager	X *				
Section 104 – reports by skilled persons	X **				
Section 106 – interview					X
Sch 12 paragraph 2 – entry and inspection without a warrant	X ***				
Sch 12 paragraph 4 – audit	X				
Sch 12 paragraphs 5-7 – entry and inspection with a warrant	X ***				

* Where provider is an entity.
** May be required to appoint a skilled person and must give the skilled person all such assistance as they may reasonably require.
*** Premises used by the provider of a regulated service in connection with the provision of a regulated service and any person on the premises.

3. Ofcom's general approach to online safety information gathering

3.1 This section explains Ofcom's general approach to information gathering and addresses issues that are common to the exercise of all our information gathering powers under the Act. It covers:

a) why Ofcom uses statutory information gathering powers;
b) Ofcom's general duties when exercising information gathering powers;
c) how we will use our information gathering powers, including:
    i) exercising our powers in a proportionate way;
    ii) information provided voluntarily;
    iii) using information for a different purpose;
d) record retention and personal data;
e) confidential information;
f) disclosure of information, including:
    i) circumstances in which we may disclose information that we have gathered;
    ii) the process we expect to follow if we propose to disclose information; and
    iii) freedom of information requests;
g) information security; and
h) service of notices.

Why Ofcom uses statutory information gathering powers

3.2 In order to exercise our functions in a way that is effective and proportionate, we need to ensure that our regulatory decisions are founded on a robust evidence base. Information held by stakeholders is often fundamental to a proper appreciation of the factual, economic and legal context within which we exercise our regulatory functions.

3.3 The statutory information gathering powers conferred on Ofcom by Parliament pursuant to the Act are an important tool by which we can obtain information from stakeholders in support of our online safety functions.

3.4 These powers enable us to address the information asymmetry that may exist between Ofcom and stakeholders active in the sectors we regulate and to discover, obtain and use information from stakeholders to take what we consider to be the best possible decisions. Our information gathering powers also allow us to compel the provision of certain information that stakeholders might not otherwise wish to provide, for instance when considering the case for regulation in the interests of citizens and consumers, monitoring and understanding market developments, supervising regulated services, and investigating suspected compliance failures.

3.5 Wherever possible, Ofcom will draw from existing internal and external information sources to avoid unnecessary duplication of effort and to minimise the burden placed

on those from whom information is requested. However, there will remain specific areas where it is necessary to collect additional information. Where our regulatory activities are dependent on information held by stakeholders, using our statutory information gathering powers helps us obtain information and gain an evidence base which is accurate, robust and complete.

Ofcom's general duties when exercising information gathering powers

3.6 When exercising our information gathering powers, we will act in accordance with our principal duties as set out in section 3 of the Communications Act 2003 (the 'Communications Act'), which are:

a) to further the interests of citizens in relation to communications matters; and
b) to further the interests of consumers in relevant markets, where appropriate by promoting competition.

3.7 In addition, under the Act we are required to secure a number of objectives, including the adequate protection of citizens from harm presented by content on regulated services, through the appropriate use by providers of such regulated services of systems and processes designed to reduce the risk of such harm (section 3(2)(g)).

3.8 In our work to secure this objective, we must have regard to the matters in section 3(4A) of the Communications Act to the extent they appear to us relevant. These include:

a) the risk of harm to citizens presented by content on regulated services;
b) the need for a higher level of protection for children than for adults;
c) the need for it to be clear to providers of regulated services how they may comply with their duties under the Act; and
d) the extent to which providers of services demonstrate, in a way that is transparent and accountable, that they are complying with their duties under the Act.

3.9 We must also have regard to the matters in section 3(3) and (4) of the Communications Act (to the extent relevant in the circumstances). These include a requirement to have regard to the principles under which our regulatory activities are transparent, accountable, proportionate, consistent, and targeted only at cases in which action is needed.

How we will use these powers[5]

We will exercise our powers in a proportionate way

3.10 We will consider on a case-by-case basis whether exercising an information gathering power would be proportionate, in line with our regulatory principles to seek the least

[5] This sub-section discusses how we will approach our discretion to exercise our information gathering powers. We have a duty, rather than a discretion, to issue a Data Preservation Notice where certain statutory criteria are fulfilled. We discuss this further in Section 4.

intrusive regulatory methods of achieving our objectives.[6] When faced with a choice of which of our information gathering powers to use, we will typically exercise the power that imposes the least burden on stakeholders without compromising our ability to fulfil our objectives.

3.11 The decision to exercise an information gathering power will be taken by a person with appropriate delegated authority from Ofcom's Board.[7]

3.12 In reaching our decision about whether to exercise an information gathering power, we will generally take account of a range of factors in the round including:

a) the regulatory purpose for which we need the information;
b) the feasibility and cost to the stakeholder involved in collating the information, including the size or capacity of that stakeholder and the resources required to provide the information;
c) the use for which we intend to rely on the information and the extent to which we need to be able to rely on robust and reliable evidence;
d) the resources Ofcom will need to gather and process the information;
e) whether the information is available from other sources or could be provided voluntarily (including whether the information may already be held by Ofcom, and if so, whether we consider we need it in a different format);
f) any other potential costs or other impacts on the person who would be subject to the power or other relevant persons, for example, the cost of appointing a skilled person or carrying out an audit or impacts on a person's right to privacy in relation to the information we are seeking.
g) where relevant, and taking into account relevant factors above, whether it may be appropriate to:

i) send the same statutory information notice to all stakeholders of a particular type;
ii) only send a statutory information notice to a sub-set of those stakeholders; and/or
iii) send a smaller or adapted set of questions to some stakeholders.

3.13 However, in certain circumstances we will generally obtain information using our statutory powers, including:

a) where we intend to rely on information provided by a stakeholder in published documents such as consultations and statements; and
b) where information will be relied on to make decisions in the context of an investigation or to make a decision that imposes requirements on a stakeholder.

3.14 Where information that we intend to rely on as part of our decision-making has been provided on a voluntary basis, we generally expect to use our statutory powers to confirm the information is accurate and complete, to ensure that our evidence base is reliable and robust.

[6] Ofcom may only issue information notices under sections 100(1) or 101(1) in a way that is proportionate to the use to which the information is to be put in the exercise of Ofcom's functions: see sections 100(4) and 101(4). Further, in performing its principal duties under section 3(1) of the Communications Act, Ofcom is required to have regard to the principles under which regulatory activities should be (amongst other things) proportionate: see section 3(3)(a).
[7] This is typically a project director but in certain circumstances, other appropriately senior colleagues have delegated authority to exercise these powers.

3.15 We may also issue a statutory information notice when requesting user or other information that may be commercially sensitive, including where a stakeholder asks us to request the information formally.

3.16 As explained below, where we exercise our information gathering powers, we will explain why we need the requested information.[8] Where appropriate, we may also explain to stakeholders the criteria we used to determine the type or sub-set of stakeholders that have been sent a statutory information notice.

3.17 When exercising our information gathering powers we will, to the extent possible, take account of any legislation which may restrict the ability of a stakeholder to provide certain information to us. However, it will be the responsibility of the person subject to the information power to draw any such legislation to our attention and to explain how it restricts the recipient's ability to respond.

3.18 Ofcom's powers to require information do not apply to information in respect of which a claim to legal professional privilege, or (in Scotland) to confidentiality of communications,[9] could be maintained in legal proceedings (in the remainder of this document we refer to this as legally privileged information for convenience). Where a stakeholder withholds information that Ofcom has requested on the basis that this information is privileged, they should provide Ofcom with a summary of the nature of the information and an explanation of why they consider it to be privileged.

3.19 If a stakeholder is concerned about the proportionality of the exercise of our statutory information gathering powers, they are encouraged to raise this in writing (with an accompanying explanation) with the responsible director,[10] copying the Information Registry,[11] including in response to any draft statutory information notice.[12]

Information provided voluntarily

3.20 It is not always appropriate for us to gather information using our statutory powers. We often benefit from the provision of information from stakeholders on an informal or voluntary basis and from a constructive dialogue in relation to a range of issues. We particularly welcome engagement from stakeholders in what are often complex, technical matters. Examples of when we may consider it appropriate to obtain information on an informal or voluntary basis include but are not limited to:

a) When gathering information for more general or monitoring purposes where we do not intend to rely on the information in a published document, in the context of an investigation or in a decision that imposes requirements on a stakeholder.

---

[8] In relation to many of our information gathering powers, the Act requires us to set the purpose for which we require the requested information, e.g. s 102(3)(b) in relation to information notices.

[9] This covers 'legal advice privilege' (which attaches to a particular communication or document if the dominant purpose of that communication or document was to obtain or give legal advice) and 'litigation privilege' (which relates to communications between a person and their lawyer (or between the person or their lawyer and a third party) made at the stage when litigation is pending or in contemplation, and only when made for the sole or dominant purpose of conducting that litigation). Information is not legally privileged solely because it has been sent to or from a lawyer.

[10] Typically, a project director is responsible for deciding whether to exercise an information gathering power (including whether it is proportionate) but in certain circumstances, other appropriately senior colleagues have delegated authority to exercise these powers.

[11] We explain the role of the Information Registry below.

[12] We discuss draft statutory information notices below.

b) When gathering background or preliminary information to help facilitate our understanding of a particular area or issue, in particular where we welcome the views or opinions of stakeholders rather than require the provision of information or documentary evidence (or explanations of documentary evidence) based on objective facts.

3.21 If we intend to rely on information provided by a stakeholder on a voluntary basis in certain circumstances, we generally expect to use our statutory powers to confirm that information is accurate and complete. This should ensure our decisions are based on robust and non-biased evidence. Additionally, if we have been told informally that certain information is not available (or, where relevant, cannot be generated), we may also use our statutory powers to obtain formal confirmation of this (or, where relevant, require stakeholders to generate or obtain the requested information).[13]

3.22 If we consider any part of a response to a statutory information notice is unclear, or the question does not appear to have been answered fully, we may issue one or more clarification questions. While requests for clarification may not be contained in a new statutory information notice, they should not be treated as an informal or voluntary request; a response to a clarification question is treated as a response to the relevant question in the associated statutory information notice, meaning we can take enforcement action for failing to comply with a request for clarification.

3.23 Where we exercise our information gathering powers, we will explain why we need the required information.[14]

Using information for a different purpose

3.24 Where we have obtained information for a specified purpose and wish to use that information for a different purpose, we will generally send the recipient another statutory information notice requiring the same information to be provided for the new purpose.

3.25 In some circumstances, we may, as an alternative, consider it appropriate to explain why we need to use the information for a different purpose and ask for the recipient's consent to use it for this new purpose. If the recipient does not give consent then we may send a statutory information notice requiring the same information to be provided for the new purpose.

3.26 When seeking to use information previously provided for a different purpose, we may also ask the recipient to confirm the information previously provided remains up-to-date and, where relevant, to provide updated information. We will generally do this in another statutory information notice.

Confidential information

3.27 For the purposes of this Guidance, confidential information means information that relates to the affairs of a body or private affairs of an individual, the publication of

[13] See, for example, section 100(2)(a) of the Act, which provides that Ofcom may require certain people to obtain or generate information in certain circumstances.

[14] In relation to many of our information gathering powers, the Act requires us to set the purpose for which we require the requested information, e.g. s 102(3)(b) in relation to information notices.

which would or might seriously and prejudicially affect the interests of that body or individual.[15]

3.28 Where requested in a statutory information notice, recipients must provide the information requested, even if they consider that the information, or any part of it, is confidential (for example due to its commercial sensitivity). Recipients should clearly identify any such confidential information and explain in writing their reasons for considering it confidential, for example, the reasons why they consider disclosure of the information will seriously and prejudicially affect the interests of their business, a third party or the private affairs of an individual.

3.29 Ofcom will take into account any representations made by recipients that certain information should be considered confidential. However, it is for Ofcom to decide what is or is not confidential, taking into account any relevant common law and statutory definitions. We do not accept unjustified or unsubstantiated claims of confidentiality. Blanket claims of confidentiality covering entire documents or types of information are also unhelpful and will rarely be accepted. For example, we would expect stakeholders to consider whether the fact of the document's existence or particular elements of the document (e.g. its title or metadata such as to/from/date/subject or other specific content) are not confidential. Recipients should therefore identify specific words, numbers, phrases or pieces of information they consider to be confidential.

3.30 Any confidential information provided to Ofcom is subject to restrictions on its further disclosure under the common law of confidence. In many cases, information provided to Ofcom is also subject to statutory restrictions relating to the disclosure of that information (regardless of whether that information is confidential information).[16] Our general approach to the disclosure of information is set out below.

Disclosure of information

Circumstances where we may disclose information that we have gathered

General

3.31 We will not disclose information we have gathered from stakeholders unless:

a) we have consent;
b) we are required by a court or tribunal to disclose the information in relation to civil or criminal proceedings; or
c) there is another legal basis for us disclosing the information, and we consider it is proportionate to disclose the information in the circumstances.

3.32 Where we have gathered information relating to a particular business using our information gathering powers, section 393 of the Communications Act explains that Ofcom cannot disclose that information without the consent of the person carrying on that business, unless this is permitted for specific, defined purposes (and in many cases only to specific persons), as set out in sub-sections (2) to (7). One of those purposes is where we consider disclosure necessary for the purpose of facilitating the exercise of

[15] Section 149 of the Act.
[16] For this reason, we do not generally consider it necessary to sign non-disclosure agreements.

our online safety functions. It is a criminal offence for a person to disclose information in contravention of section 393.[17]

3.33 The general restriction under section 393 of the Communications Act does not apply in certain circumstances, including:

a) where Ofcom is publishing a report under the Act or is arranging for the publication of its advice to the Secretary of State as to the categorisation of regulated user-to-user services and regulated search services. In these circumstances, Ofcom must have regard to the need to exclude from publication, so far as practicable, confidential information;[18]
b) when Ofcom is publishing details of enforcement action under the Act. In this circumstance, Ofcom may not publish confidential information.[19]

3.34 Ofcom will generally redact information identified as confidential from our publications or withhold it from the disclosures we make. However, for the avoidance of doubt, we may disclose such information where permitted by law. For example, Ofcom may disclose information to facilitate the carrying out of our functions by ensuring stakeholders can properly understand the basis for our reasoning.[20] We set out from paragraph 3.41 below the process we expect to follow if we propose to disclose information, including information identified as confidential.

3.35 In some cases, we may decide not to publish certain information, even where it is not confidential. For example, we may decide not to publish distressing material such as narratives about suicide, on the basis that this could cause undue distress and would not facilitate the exercise of our functions.

Disclosure to overseas regulators

3.36 The Act also enables Ofcom to co-operate with an overseas regulator listed in regulations made by the Secretary of State, including by disclosing 'online safety information',[21] for certain purposes. Those purposes are:

a) to facilitate the online safety functions of the overseas regulator which correspond to Ofcom's functions under the Act (the 'online regulatory functions'); or
b) criminal investigations or proceedings relating to a matter to which the overseas regulator's online regulatory functions relate.[22]

3.37 Only the Secretary of State can decide which overseas regulators Ofcom has the power to disclose information to under this mechanism.[23]

---

[17] Section 393 of the Communications Act (general restrictions on disclosure of information), see Section 115 of the Act, Part 4, Chapter 4
[18] In the case of a report, see section 393(6)(b) of the Communications Act and section 164 of the Act. In the case of Ofcom's advice, see section 393(6)(a) of the Communications Act and Schedule 11, paragraph 4, to the Act.
[19] See section 393(6)(a) of the Communications Act and section 149 of the Act.
[20] Our regulatory activities should also be transparent and accountable (section 3(3)(a), Communications Act).
[21] 'Online safety information' is defined as information held by Ofcom in connection with any of Ofcom's online safety functions: section 114(7) of the Act.
[22] Section 114(1) of the Act.
[23] Section 114(2) of the Act, which gives the Secretary of State the power to make secondary legislation setting this out, which must be passed by the UK Parliament. See The Online Safety (List of Overseas Regulators) Regulations 2024.

3.38 The Secretary of State may update this list over time.

3.39 The Act puts in place various safeguards concerning the overseas regulator's treatment of the information that Ofcom discloses. Where Ofcom discloses information to an overseas regulator, they may not:

a) use the information for a purpose other than the purpose for which it was disclosed; or
b) further disclose the information;

without Ofcom's consent or in accordance with an order of a court or tribunal.[24]

3.40 The Act also puts in place various limitations on Ofcom's power to disclose information to an overseas regulator, including that Ofcom may not make a disclosure that would contravene data protection legislation.[25]

The process we expect to follow if we propose to disclose information

3.41 When deciding whether to disclose information we will carefully balance the need to disclose the relevant information against any concerns or objections raised by the person who provided the information in relation to its disclosure.

3.42 We may have explained our intention to disclose information in any draft or final statutory information notice. If we have not and subsequently propose to disclose information, we will normally first explain our intention to disclose the information (including the context in which we intend to disclose it) and give that person the opportunity to make representations about the proposed disclosure.[26] There may be circumstances where this is not appropriate, for example where we are disclosing information to an overseas regulator for the purpose of an overseas criminal investigation relating the overseas regulator's online regulatory functions and giving notice of our intention to disclose the information to the overseas regulator could prejudice their investigation.

3.43 We will generally try and resolve any objections to a proposed disclosure through constructive dialogue. If we remain of the view that we need to disclose the information and the person concerned continues to object, we will give them advance warning prior to making the disclosure. This will give the person concerned an opportunity to challenge our decision or raise the issue with the Procedural Officer, where relevant.[27]

3.44 Where Ofcom decides the information provided does not need to be disclosed in full but considers it appropriate to include some information in a proposed disclosure, we may ask the person concerned to provide a summary of information or a range of

[24] Section 114(3) of the Act.
[25] Section 114(5)(b) of the Act.
[26] As noted at paragraph 4.86 below, where we issue a Data Preservation Notice we generally disclose the recipient's response to the coroner without further notice. Similarly, as noted at paragraphs 4.93 and 4.103 below, where we issue a draft or final Coroner Information Notice, we will generally disclose the recipient's comments on the draft, or their response to the final notice, without further notice.
[27] Section 10 of our Online Safety Enforcement Guidance explains when a procedural complaint can be referred to Ofcom's Procedural Officer and the process for doing so.

numbers for the purposes of including this in the relevant disclosure, rather than simply removing the information.

3.45 Where in order to exercise our functions under the Act there is a need to disclose information regularly, a different process for disclosing information may be appropriate. Where we intend to take a different approach to that set out in this policy, we would expect to explain our approach to stakeholders in advance of disclosing any information.

3.46 Our Online Safety Enforcement Guidance provides further information about our approach to disclosing confidential information during an investigation. This would apply to information we have obtained for the purposes of an investigation using our information gathering powers.

Freedom of information requests

3.47 As a public authority, Ofcom is subject to the Freedom of Information Act 2000 (the 'FOI Act') meaning it has a general duty to provide access to information that is requested by a third party. However, a number of exemptions may apply in which case Ofcom is not required to disclose the requested information.[28] The applicability of any exemption will depend on the nature of the information sought by any FOI request made.

3.48 In particular, section 44 of the FOI Act exempts information from disclosure if its disclosure is prohibited under another enactment.[29] This means that where we have gathered information relating to a particular business (either using our information gathering powers under the Act or on a voluntary basis), we are prohibited from disclosing that information in response to a FOI request, unless we have the consent of that business.

3.49 If we decide that we cannot disclose information because an FOI exemption applies, it is unlikely to be necessary to discuss this with the business that provided the information to us.

3.50 If we need more information to help us determine whether an FOI exemption applies, we will discuss the request with the business that provided the information to us. We are subject to statutory deadlines for responding to FOI requests and expect a prompt reply.

Record retention and personal data

3.51 As a public authority, we will need to retain information as part of the evidence base underlying any decision we reach. We will keep information in line with our records and information management policy.

3.52 We may use our information gathering powers to obtain personal data if we consider that this information is necessary and relevant for the purpose of our functions.

[28] The Information Commissioner's Office provides guidance on the exemptions that may apply.
[29] For example, where disclosure is prohibited under section 393 of the Communications Act.

Personal data is defined in section 3(2) of the Data Protection Act 2018 as information relating to an identified or identifiable living individual.[30]

3.53 In general, our role under the Act focuses on tackling the root causes of online content that is illegal or harmful to children, by improving the systems and process that services use to address them. Consistent with that role, in many cases it will not be necessary to use our statutory information gathering powers to obtain personal data to enable us to perform our online safety functions. However, there may be circumstances where obtaining personal data is necessary. For example, where we obtain emails or meeting minutes from a service provider, this may include the names or email addresses of individuals employed by that provider, where these are relevant. In addition, there may be occasions where we consider it necessary to obtain personal data related to users of a service. For example, where a coroner has requested from Ofcom information about content encountered by a deceased child, and Ofcom has decided to exercise its power under s101(1) to issue a Coroner Information Notice to require a service provider to provide such content, that content may, depending on the case, include personal data related to other living users.

3.54 In all cases, Ofcom will seek to limit the personal data which it requires under its information gathering powers to that which is necessary for the performance of our functions under the Act. [31]

3.55 Those subject to our information gathering powers will be responsible for complying with their own obligations under relevant data protection legislation.[32] Any personal data they process in responding to our request for information is processed by them on their own account, as a data controller, rather than as a processor of that data for Ofcom. Our information gathering powers are not capable of requiring a person to process personal data in a way that contravenes UK data protection legislation,[33] including the UK GDPR. In determining whether the processing of personal data would contravene UK data protection legislation, the duty to provide the requested information should be taken into account.[34]

3.56 Under Article 14 of the UK GDPR, where we (as data controller) have obtained personal data other than from the data subject, we must provide the data subject with certain information.[35] However, there are various exceptions to this obligation, which we will consider on a case-by-case basis. These exceptions include where providing the data

---

[30] An identifiable living individual is defined in section 3(3) of the Data Protection Act 2018. We note that while data protection law does not apply to the personal data of deceased persons, it may apply to any third-party personal data that might potentially be within scope of a Coroner Information Notice or Data Preservation Notice as discussed below. Where that is the case, providers must comply with UK data protection law.
[31] This is consistent with Article 5(1) of the UK General Data Protection Regulation (the 'GDPR') which provides for 'data minimisation', including that personal data shall be 'limited to what is necessary in relation to the purposes for which they are processed'.
[32] These obligations include that those subject to our information gathering powers must have a valid lawful basis in order to process personal data. The ICO's 'A guide to lawful basis' guidance provides further information about this, including the conditions for processing special category personal data. Those subject to our information gathering powers may find it helpful to refer to this when determining their lawful basis.
[33] See sections 100(8A) and 101(5A) of the Act in relation to information notices. UK data protection legislation means the legislation identified in section 3(9) of the Data Protection Act 2018.
[34] Under the UK GDPR, a person has a lawful basis for processing personal data if that is necessary for compliance with a legal obligation to which the controller is subject: Article 6(1)(c).
[35] UK GDPR, Article 14(1)-(3).

subject with the required information would seriously impair our ability to achieve the objectives of the processing, or would involve a disproportionate effort,[36] taking account of any measures to protect the data subject's rights, freedoms and legitimate interests.[37] In making that assessment we would not expect to disclose any personal data unless we are satisfied we have a legal basis to do so, for example, because one of the statutory gateways for disclosure applies.

3.57 Ofcom's General Privacy Statement contains further information about how Ofcom will handle personal data.

3.58 At paragraph 4.64 below we set out some further guidance regarding personal data in the context of Remote Viewing Information Notices under section 100(3).

Information security

3.59 Ensuring information is appropriately protected is central to Ofcom's work and our reputation as the UK's communications regulator.

3.60 The security of commercially confidential and sensitive personal information provided to Ofcom is taken extremely seriously. We consistently test and monitor the efficacy of our systems to protect the data we hold and ensure data is only kept in accordance with our records and information management policy.

3.61 As noted above, by virtue of section 393 of the Communications Act we are subject to a statutory restriction relating to the disclosure of information we have gathered. It is a criminal offence to disclose information in contravention of this provision. The safeguards provided by this section apply to information that Ofcom has gathered using its statutory powers in relation to other regulatory functions as well as online safety, including for example Ofcom's telecoms and broadcasting functions. This restriction applies to all information relating to a business that has been provided to us (regardless of whether it is confidential), including, for example, information generated through a test or demonstration that we have required.

Service of notices

3.62 To exercise most of our information gathering powers under the Act, we must give a notice to the person from whom we are seeking the information.[38] Where that is the case, we may give a notice to that person by:[39]

a) delivering it by hand;
b) leaving it, or sending it by post[40] to, that person's 'proper address'; or

[36] UK GDPR, Article 14(5).
[37] When relying on the 'disproportionate effort' exception, it is necessary to assess whether there is a proportionate balance between the effort involved in providing the data subject with the required information and the effect that the use of their personal data will have on them. See ICO: Are there any exceptions? | ICO.
[38] Some of our information gathering powers do not require Ofcom to issue notices. For example, it is not necessary for Ofcom to issue a notice where we exercise our powers of entry and inspection without a warrant, unless we require information to be provided, relevant documents to be produced, or a relevant test or demonstration to be performed during the inspection: see paragraphs 2-3 of Schedule 12 to the Act.
[39] Section 208(1)-(2) of the Act.
[40] Where we serve a notice by post, we will treat it as having been served at the time at which it would be delivered in the ordinary course of post, unless the contrary is proved: see Interpretation Act 1978, section 7.

c) sending it by email to the person's email address.[41]

3.63 The Act specifies what the person's 'proper address' is in different scenarios:

a) Where we are giving a notice to a person who is a **provider of a regulated service**, their proper address is any address (within or outside the UK) at which we believe, on reasonable grounds, it will come to the attention of the person, or, where the person is an entity, any director[42] or other officer[43] of that entity.[44]
b) Where we are giving a notice to a person who is **not a provider of a regulated service**, their proper address is:

i) where the person is an entity, the address of the entity's registered or principal office.[45] Where the entity is registered or carrying on business outside the UK, or with offices outside the UK, we may send the notice to (or leave it at) the entity's principal office in the UK or, if the entity has no office in the UK, any place in the UK at which we have reasonable grounds to believe that the notice will come to the attention of any director or other officer of the entity;[46]
ii) where the person is not an entity, the person's last known address.[47] In the case of a notice to an individual requiring them to attend an interview,[48] the individual's last known address is their home address or, if they are currently connected with a provider of a regulated service, the address of the provider's registered or principal office.[49]

3.64 The Act also specifies what the person's email address is in different scenarios, namely:[50]

a) any email address published for the time being by that person as an address for contacting that person; or
b) if there is no such published address, any email address by means of which we have reasonable grounds to believe that the notice will come to the attention of that person or (where that person is an entity) any director or other officer of that entity.

3.65 Where we give a notice to an entity by email:

a) we may mark the email for the attention for of the Company Secretary or other officer or director of the entity; and
b) we will consider the notice delivered even if the recipient does not acknowledge receipt, unless we receive information to the contrary (e.g. if we receive a notification that the email was undelivered). In accordance with the Act, we will treat a notice sent by email as having been served 48 hours after it was sent, unless we receive

---

[41] A notice sent electronically is treated as served 48 hours after it was sent, unless the contrary is proved: section 208(11) of the Act. For example, if the recipient acknowledges receipt 2 hours after we send the notice, then we will treat the notice as being served at that time.
[42] A director includes any person occupying the position of a director, by whatever name called: see section 208(12) of the Act.
[43] An officer, in relation to an entity, includes a director, manager, partner, associate, secretary or, where the affairs of the entity are managed by its members, a member: see section 208(12) of the Act.
[44] Section 208(6) of the Act.
[45] Section 208(7) of the Act.
[46] Section 208(8) of the Act.
[47] Section 208(7) of the Act.
[48] Under section 106 of the Act.
[49] Section 208(9) of the Act.
[50] Section 208(10) of the Act.

information proving the contrary.[51] For example, if the recipient acknowledges receipt two hours after we sent the notice, then we will treat the notice as having been served at that point in time.

3.66 Where possible, we will serve a notice electronically (by email) rather than by other means such as by post.

[51] Section 208(11) of the Act.

4. Information notices

Introduction

4.1 An information notice is a means through which we formally gather specific information. The information notice will contain a number of focused questions relating to the purpose of the request and the responses we receive help us fulfil our statutory functions.

4.2 There are a number of different types of information notices that we may issue under the Act.

4.3 **Section 100(1)** of the Act grants Ofcom the power to issue a notice requiring any person (as detailed at paragraph 4.10 below) to provide information that we require to exercise, or to decide whether to exercise, any of our online safety functions. This may include a requirement to:

a) obtain or generate information;
b) provide information about the use of a service by a named individual.

4.4 **Section 100(3)** of the Act provides that, as part of our power to issue an information notice under sub-section (1), we may require a recipient to take steps to allow a person authorised by Ofcom to remotely view certain information in real time, for example tests and demonstrations. We refer to this type of information notice as a Remote Viewing Information Notice.

4.5 **Section 101(C1)** of the Act imposes a duty on us, in certain circumstances, to require the provider of a regulated service to retain information relating to a deceased child's use of the service.[52] We also have a power to require certain others to retain such information. We refer to this type of notice as a Data Preservation Notice. A Data Preservation Notice can only require a person to retain information that we may subsequently require that person to provide pursuant to a notice issued under section 101(1) (summarised in the next paragraph).

4.6 **Section 101(1)** of the Act grants us a power to request information from providers of regulated services, and certain others, for the purpose of responding to a request for information from certain authorities in connection with an investigation into the death of a child. Those authorities are a senior coroner (in England and Wales), a procurator fiscal (in Scotland) or a coroner (in Northern Ireland). We refer to these authorities as 'Coroners' and refer to this type of notice as a Coroner Information Notice.

4.7 **Section 103** of the Act grants us a power to include a requirement in an information notice issued to a provider of a regulated service under sections 100 or 101 of the Act to name a senior manager who may reasonably be expected to ensure compliance with the requirements of the notice.

4.8 This part of the Guidance covers:

a) when we may issue information notices under section 100, and to whom;

[52] Section 101(C1), and other provisions associated with Data Preservation Notices, were inserted into the Act by section 124 of the Data (Use and Access) Act 2025.

b) Ofcom's Information Registry;
c) the typical process for receiving and responding to an information notice;
d) specific considerations for section 100 notices requiring the performance of a test;
e) specific considerations for Remote Viewing Information Notices under section 100(3);
f) specific considerations for Data Preservation Notices under section 101(C1);
g) specific considerations for Coroner Information Notices under section 101(1); and
h) requirement to name a senior manager.

When Ofcom may issue information notices under section 100, and to whom

4.9 Section 100 of the Act grants Ofcom the power to require information from certain persons by way of a statutory notice.[53]

4.10 We may issue an information notice to anyone who holds relevant information which we consider is necessary for the purpose of exercising, or deciding whether to exercise, our online safety functions.

4.11 The persons to whom we may issue an information notice under section 100 are:

a) a provider of a user-to-user service or a search service;
b) a provider of an internet service on which regulated provider pornographic content is published or displayed;
c) a person who provides an ancillary service[54] in relation to a regulated service;
d) a person who provides an access facility[55] in relation to a regulated service;
e) a person who was within any of paragraphs (a) to (d) at a time to which the required information relates; and
f) a person not within any of paragraphs (a) to (e) who appears to Ofcom to have, or to be able to generate or obtain, the information we require.[56]

4.12 We may only issue an information notice where this is proportionate to the use of the information being gathered.[57] We set out further detail about the principle of proportionality from paragraph 3.10 above.

4.13 Section 100(6) sets out a non-exhaustive list of functions for the purpose of which we may issue an information notice under section 100. These include (but are not limited to) assessing compliance with duties imposed on providers of regulated services,

[53] Section 102(1) of the Act.
[54] Under section 144(11) of the Act, a service is an 'ancillary service' in relation to a regulated service if the service facilitates the provision of the regulated service (or part of it), whether directly or indirectly, or displays or promotes content relating to the regulated service (or to part of it). These may include services which enable funds to be transferred to a regulated service, search engines which generate search results displaying or promoting content relating to a regulated service, user-to-user services which make content relating to a regulated service available to users, and services which use technology to facilitate the display of advertising on a regulated service (e.g. an ad server or ad network) – see section 144(12).
[55] Under section 146(10) a facility is an access facility in relation to a regulated service if the person who provides the facility is able to withdraw, adapt or manipulate it in such a way as to impede access (by means of that facility) to the regulated service (or to part of it) by UK users of that service. These may include internet access services by means of which a regulated service is made available and app stores through which a mobile app for a regulated service may be downloaded or otherwise accessed – see section 146(11).
[56] Section 100(5) of the Act.
[57] Section 100(4) of the Act.

preparing a code of practice, and carrying out research or preparing a report in relation to online safety matters.

4.14 As well as requiring information that is already held by the recipient, we can require a recipient to obtain or generate information, or to provide information about the use of a service by a named individual.[58]

4.15 An information notice issued under section 100 may require the production of documents wherever those documents are held, including outside the UK.[59]

Ofcom's Information Registry

4.16 To make our information gathering as efficient as possible, Ofcom's formal information notices are typically managed and coordinated by a central team: the Information Registry.[60]

4.17 The Information Registry was set up with the aim of reducing the burden on stakeholders by providing a central contact point, streamlining our activities and ensuring better oversight and coordination of information requests.

4.18 The Information Registry supports project teams across Ofcom by preparing, issuing and tracking information requests and gathering responses, ensuring requests use clear and consistent terminology and are prepared to a high standard.

4.19 To ensure efficiency and to minimise the regulatory burden placed on stakeholders to the extent possible, the Information Registry will record and have oversight of the number of information notices which have been sent to a recipient at any one time. This helps ensure we set reasonable deadlines for stakeholders to respond and can consider the burden placed on stakeholders in the round when considering whether to issue requests.

4.20 The Information Registry maintains up-to-date external stakeholder information, including contact details and corporate structure information.

4.21 Finally, the Information Registry is responsible for collating and tracking responses, ensuring that responses to formal information notices are complete, accurate and submitted within the stipulated deadline. This ensures we are able to make effective decisions based on accurate, reliable and complete information while minimising the burden placed on stakeholders wherever possible. The Information Registry may escalate failures to respond to statutory information notices to Ofcom's Enforcement team for further action where appropriate.

How the Information Registry works with stakeholders

4.22 As a central point of contact between external stakeholders and project teams, the Information Registry stays up to date with information gathering activities to identify peaks and manage them effectively where it is possible to so.

[58] Sections 100(2)(a) and (b) of the Act.
[59] Section 204(2) of the Act.
[60] Further information on the Information Registry and our statutory information gathering processes can be found on the Ofcom website.

4.23 The team continuously seeks to ensure that Ofcom's information gathering activities are transparent and consistent. Where necessary, the Information Registry will meet regularly with external stakeholders[61] to provide visibility of the timing of upcoming statutory information notices.

4.24 The Information Registry acts as a central point of contact for all stakeholders for general advice on information gathering and queries about specific notices. It will also support stakeholders that may be unfamiliar with the process and can offer introductory meetings to new or smaller stakeholders where required.

Typical process

Draft statutory information notices

4.25 Ofcom will, as a general rule, issue statutory information notices in draft form to the stakeholder holding the relevant information to ensure that the notice is appropriately worded and targeted and sufficiently clear for the recipient to respond within the proposed timeframe.

4.26 Where Ofcom issues a statutory information notice in draft, we will allow an appropriate period of time for comment on the information or data required by the notice, as well as the practicality of providing the information in the proposed timescales. We will take into account any comments on the draft statutory information notice and decide whether we consider it appropriate to confirm or amend the draft notice before issuing it as a final version.

4.27 However, there are times when it is likely to be appropriate to issue statutory information notices without issuing a draft request to the recipient first.[59] These include but are not limited to:

a) where it is a simple request or the request is for standard information known to be held by stakeholders, such as turnover numbers or basic customer information;
b) where we issue a Data Preservation Notice, as it is important to issue this as quickly as possible so that it is more likely to be successful in preserving the relevant information. Further, if the child to which the notice relates did not have an account with the service in question, or the recipient does not hold any information of the kind required to be retained, the recipient may respond to a notice explaining this;
c) when we are exercising our enforcement functions, where prior notice of a statutory information notice (i.e. a notice in draft) may not be appropriate due to concerns relating to the destruction of documents;
d) where information has been provided to Ofcom previously on an informal/voluntary basis or where we need to re-obtain information previously provided in response to a statutory information notice to use for a different purpose;
e) where we are issuing a similar statutory information notice to a large number of stakeholders, such that preliminary engagement is not practicable;
f) where we are asking for updates to information previously provided, where questions are the same as, or very similar to, questions previously asked;

[61] The Information Registry generally meets regularly with those external stakeholders who receive significant numbers of statutory information notices each year, and on a more ad hoc basis with stakeholders receiving fewer statutory information notices.

g) any other scenario in which Ofcom does not consider it appropriate to issue a statutory information notice in draft in the specific circumstances of the case.

Service of the notice

4.28 Paragraphs 3.62 - 3.66 above set out guidance regarding how we will serve notices, including information notices.

Contents of a statutory information notice

4.29 An information notice (other than a Data Preservation Notice, which is discussed at paragraphs 4.72 below) will specify or describe:

a) the information being requested;
b) why the information is needed by Ofcom;
c) the form and manner in which the information should be provided;
d) the deadline by which the information should be provided; and
e) the consequences of not complying with the notice.

Complying with a statutory information notice

Recipients must provide complete and accurate information

4.30 The recipient of a statutory information notice is under a legal duty to act in accordance with the requirements of the notice, and to ensure that complete and accurate responses are provided to all questions by the deadline.[62] The consequences of a failure to comply with the powers set out in this section could include:

a) enforcement action by Ofcom; or
b) criminal liability.

4.31 Section 8 of this Guidance sets out the consequences of non-compliance with our information gathering powers in more detail.

4.32 On receipt of a statutory information notice, the recipient should:

a) review the request and **acknowledge receipt** of it to Ofcom;
b) carefully **read the requirements of all questions** (including any applicable definitions) and ensure they understand what is being requested. If the recipient does not understand any aspect of the notice, or has any questions about the notice or the obligations it places on the recipient, they should contact the Information Registry as soon as possible;
c) consider the response and **locate or generate any information required (or required to be retained)**, well in advance of the deadline to leave time for any issues to be resolved and for the information to be checked prior to sending it; and
d) consider all systems and places where the requested information may be stored and **carry out appropriate searches** for the information; and
e) in the case of a Data Preservation Notice, take steps to ensure the retention of any information referred to in the notice.

4.33 Before the recipient sends its response to Ofcom, they should make sure that:

[62] Section 102(8) of the Act.

a) **they have provided a response to every question** (including all sub-parts to a question) and that this response answers the question asked. If the recipient does not have some or all the information requested, they should explain why and describe what searches have been carried out to check whether the information is available to them.
b) the response is be **provided in the format requested**, for instance this might be a document in .docx format or a spreadsheet in .csv format. We generally only accept information returned in the format requested;
c) all responses provided are **clear, complete, and accurate**. If the recipient has any doubts about the accuracy of the information in their response, they should clearly explain any problems to Ofcom and provide the information with appropriate caveats. A response can refer to other documents held by Ofcom, but it should not require us to interpret a response by reference to other information or documents to understand the intended meaning.

4.34 The recipient should check the completeness and accuracy of the information provided prior to responding to the notice. For established businesses, an appropriate governance check should also be completed to ensure all responses are properly interrogated, cross-checked and reviewed through appropriate governance channels, including being signed off by an appropriate senior manager, prior to submission.[63]

Response by the required deadline

4.35 The recipient must send the response by the deadline stipulated in the statutory information notice. If the recipient does not think it can provide a response by the deadline set, it should inform us immediately and explain why. Deadlines are likely to have been set taking into account any pre-engagement with stakeholders and/or comments on draft statutory notice. We will therefore only agree to extend deadlines where there is good reason for doing so, like the unexpected absence of a key employee responsible for obtaining the required information, technical difficulties, or other exceptional circumstances beyond the recipient's control. Every extension request will be considered on its own merits.

4.36 There may be times where we require information quickly and so we may ask for the information to be provided in a phased approach. This will allow the recipient more time to provide information that may take longer to arrange (for instance, information that may need to be generated), and shorter timeframes for information that may be quicker to collect or produce.

Cancelling a statutory information notice

4.37 We may cancel a statutory information notice by giving notice to the recipient.[64] When doing so, Ofcom will confirm that no further action is needed.

[63] We would take into account any failure to carry out an appropriate governance check when considering potential enforcement action for an incomplete or inaccurate response. See Section 8 relating to failure to comply with a statutory information notice.
[64] Section 102(9) provides that Ofcom may cancel an information notice by notice to the person to whom it was given. Where Ofcom has issued a Data Preservation Notice it has a duty to cancel the notice in the circumstances specified in section 102(9A), which is discussed below.

Specific considerations for section 100 notices requiring the performance of a test

4.38 As part of an information notice under section 100(1), Ofcom may require the recipient to generate information.[65] We may require the recipient to do this by performing a test of relevant systems, processes or features, including functionalities and algorithms used by the service.[66] For example, empirical tests are a method for understanding algorithms and involve observing the output under specific conditions, e.g. by measuring the performance when processing a test dataset.

4.39 As is the case with all information notices, we may only issue an information notice requiring the performance of a test where this is proportionate to the use of the information being gathered.[67] We set out further detail about the principle of proportionality from paragraph 3.10 above.

4.40 Where we issue an information notice which requires the recipient to perform a test, we may also include a requirement under section 100(3) to take steps to enable a person authorised by Ofcom to remotely view information generated by the performance of the test in real time i.e. a Remote Viewing Information Notice. In other words, an information notice which requires the performance of a test may, or may not, include a remote viewing requirement under section 100(3).

4.41 From paragraphs 4.51 below we provide further information about Remote Viewing Information Notices. The following paragraphs address some specific considerations relevant to the performance of a test, which apply equally whether or not the information notice includes a remote viewing element under section 100(3). Those considerations are:

a) the parameters of the test;
b) test datasets;
c) test environments; and
d) information generated by the test.

Parameters of the test

4.42 We will typically outline, in the information notice, the parameters of the test that we are requiring the recipient to perform. The nature and level of detail of these parameters may vary depending on the particular case. We will generally discuss proposed parameters with the recipients (by, for example, issuing the notice in a draft) to ensure they are clear.

4.43 We do not expect to require providers to conduct open-ended or continuous tests or demonstrations. We will limit the duration of tests or demonstrations to that which is necessary and proportionate. However, in some circumstances it may be necessary to re-run a test or demonstration at a later date. For example, we may wish to assess the

[65] Section 100(2)(a) of the Act.
[66] Sections 100(1)-(2) do not explicitly provide that Ofcom is empowered to require the performance of a test or demonstration. However, section 100(3)(b) refers to 'information generated by a service … by the performance of a test or demonstration of a kind required under subsection (1)'. Therefore our power under section 100(1) includes a power to require the recipient to perform a test or demonstration.
[67] Section 100(4) of the Act.

effectiveness of any remedial action taken in response to a specific compliance concern.

Test datasets

4.44 We would generally expect to require a recipient to conduct a test using a test dataset the parameters of which are set out by Ofcom in the information notice. This would ensure that the outputs are relevant to the specific function that we are exercising or considering exercising. In most cases, Ofcom will discuss the criteria for test datasets with services in advance of conducting a test or demonstration.

4.45 We may ask a recipient to conduct a test using a test dataset provided by Ofcom.[68] We are more likely to take this approach in cases where we are conducting testing in relation to particular content or user characteristics e.g. for the purpose of testing the effectiveness of a service's technology for detecting a particular kind of illegal content. In this circumstance, we are likely to provide the test dataset in advance of any test via a secure file-sharing mechanism. We may also securely protect these datasets via password to ensure the efficacy, reliability and credibility of the test.

4.46 Ofcom may alternatively request that a regulated service conducts a test using a dataset derived from its service. If so, it is likely that we would specify, in the information notice, the criteria for identifying or generating this dataset, for example a dataset containing a representative sample of users from certain specified demographics. We are likely to take this approach in circumstances where Ofcom does not hold or cannot assemble a dataset that is likely to yield results that are relevant to the function we are exercising or considering exercising, for example datasets that includes content that, in the service's view, are prohibited by its terms of service.

Test environments

4.47 Some recipients (e.g. some regulated services) may utilise 'test environments' which are dedicated servers for testing software applications. These allow the services to evaluate the performance and impact of systems, processes or features, including functionalities and algorithms. Where a test environment is available, we expect to request that a test or demonstration is undertaken on this environment unless there are specific reasons why this would not be feasible or appropriate in a given case. We expect such cases to be exceptional.

4.48 However, if a test environment is unavailable or unsuitable, we may request the performance of a test using the server that is used to deliver the 'live' service. This could involve using either a test dataset which is derived from the service or one that is not. A test using the server used to deliver the 'live' service might impact the 'live' service being delivered to users. For example, a test or demonstration conducted on the server used to deliver the 'live' service may have limited impacts on user experience, such as increased latency. We will only take this approach where we are satisfied that it is proportionate (in accordance with the principles set out from 3.10), taking account of the potential impact on users.

[68] We note that, in relation to section 100(3) of the Act, the Explanatory Notes to the Online Safety Act 2023 state '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'.

4.49 Where we request the performance of a test (either using the server that is used to deliver the 'live' service or a dedicated test server), any data processing by the recipient of the notice would need to comply with data protection law. [69]

Information generated by the test

4.50 Where we have issued an information notice which requires the recipient to generate information by performing a test, the recipient must provide to Ofcom the information generated in accordance with the parameters set by Ofcom in the notice. This will typically be the outputs of, or the results of, the test.

4.51 In most cases, we expect to require recipients to provide information generated by a test or demonstration in a high-level, aggregate form, as specified in the notice. For example, it may include data that has been summarised, statistical averages, percentages and/or totals. In this context, we do not expect to typically require the provision of personal data (e.g. that of users of a service). As noted at paragraph 3.54, we will seek to limit the personal data which we require to that which is necessary for the performance of our functions under the Act. Further, as noted at paragraph 3.17, we will, to the extent possible, take account of any legislation that may restrict the recipient's ability to respond to an information notice.

Specific considerations for Remote Viewing Information Notices under section 100(3)

4.52 The Act places several duties on regulated services regarding the algorithms used to deliver their services. For example, the duties under the Act require user-to-user services to use proportionate measures to mitigate the risk of individuals encountering illegal content and content that is harmful to children, including measures regarding the design of algorithms. There are other duties imposed by the Act which do not explicitly refer to algorithms but where services may, in practice, use algorithmic systems to ensure compliance.

4.53 In exercising our functions under the Act, we may therefore need to gather information about those algorithms and functionalities, including by viewing information in real time where we consider it proportionate to do so.

4.54 As part of our power to issue information notices under section 100, we may issue a Remote Viewing Information Notice which requires the recipient of the notice to take steps so that a person authorised by Ofcom is able to remotely view:

a) information demonstrating in real time the operation of systems, processes or features, including functionalities and algorithms used by a service, and
b) information generated in real time by the performance of a test or demonstration of a kind required by the information notice. [70]

4.55 The person (or persons) authorised by Ofcom to remotely view this information will be authorised in writing by a person with appropriate delegated authority from the Ofcom Board.

[69] Under the UK GDPR, a person has a lawful basis for processing personal data if that is necessary for compliance with a legal obligation to which the controller is subject: Article 6(1)(c).
[70] Section 100(3) of the Act.

4.56 We may only issue a Remote Viewing Information Notice to:

a) a provider of a regulated service; or
b) a provider of an ancillary service or access facility in relation to a regulated service.[71]

4.57 As is the case with all information notices, we may only issue a Remote Viewing Information Notice where this is proportionate to the use of the information being gathered.[72] We set out further detail about the principle of proportionality from paragraph 3.10 above.

4.58 We note that Ofcom also has a separate power, as part of an audit, to require the provider to assist an authorised person to view information demonstrating in real time the operation of systems, processes or features, and/or information generated in real time by the performance of a test or demonstration (see section 7 below).[73] Further, Ofcom's power to enter and inspect premises without a warrant includes a power to view, using equipment or a device on the premises, information generated in real time by the performance of a test or demonstration. However, Ofcom's power to view this information as part of an audit, or an inspection without a warrant, is limited to viewing this information using equipment or a device on the premises in the United Kingdom. In contrast, Ofcom may issue a Remote Viewing Information Notice even in circumstances where the recipient does not have premises in the United Kingdom.[74]

4.59 When considering whether to issue a Remote Viewing Information Notice, we may take the following factors into account (in addition to the factors set out in section 3 above):

a) the complexity of the systems, processes or features that Ofcom is considering, or of the test or demonstration that Ofcom requires to be performed;
b) the location of the entity in question. For example, where the entity does not have premises in the UK, issuing a Remote Viewing Information Notice is likely to be the only way in which Ofcom can view in real time the operation of systems, processes or features, and/or information generated in real time by the performance of a test or demonstration;
c) the other information gathering powers that we could use to achieve our objectives, and the costs and impacts of those other powers on the entity in question. For example, even where an entity does have premises in the UK, it may be more proportionate to issue a Remote Viewing Information Notice than exercising the audit power or conducting an inspection without a warrant; and
d) any technical or operational limitations on viewing information, including the use of cybersecurity measures such as encryption.[75]

---

[71] Pursuant to section 100(3) of the Act, Ofcom may only exercise this power in relation to a person falling within sections 100(5)(a)-(d).
[72] Section 100(4) of the Act.
[73] See Schedule 12, paragraph 4(2)(e)-(f)). We are aware that some stakeholders may refer to algorithmic assessments as an 'audit'. However, in the context of the Act, the term 'audit' has a specific meaning; Ofcom has a power to conduct an 'audit' under Schedule 12 to the Act which is described below and which gives Ofcom the power to do certain things on premises in the UK.
[74] Provided that the recipient is a person referred to in section 100(5)(a)-(d).
[75] In relation to section 100(3) of the Act the Explanatory Notes to the Online Safety Act 2023 state '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'.

4.60 We do not expect to issue a Remote Viewing Information Notice as often as we expect to exercise our more general information notice powers under section 100. The use of this power will typically be reserved for more serious or complex cases.

4.61 We generally envisage that it will be sufficient for us to conduct remote viewing via a simple 'screen sharing' mechanism, for example using a video calling application.

Demonstrations and tests

4.62 Where, as part of a Remote Viewing Information Notice, we require the performance of a test or demonstration, the considerations set out above in relation to the performance of a test or demonstration will apply.

4.63 Given that our power is limited to remotely viewing information generated by the performance of a test or demonstration, we will not be able to directly control the service, even where we are requiring the performance of a test using the 'live' service environment. Nor could we require companies providing infrastructure services to create the means to weaken or circumvent cybersecurity measures such as encryption.[76] We will not be able to directly alter any aspect of the service or testing infrastructure, as any test required by Ofcom would be performed by the employees of the service itself. Where we require that a test be performed using the 'live' service environment (see paragraph 4.47 above), which might impact the 'live' service being delivered to users, we will only be able to view such a test and any data processing would need to comply with data protection law. We would expect to communicate regularly with the service's employees during the process of remotely viewing a test or demonstration.

4.64 In some cases, we may decide to make a recording of a test or demonstration that we remotely view, but we would only do this where it is necessary and proportionate to do so and in line with data protection requirements.

Data protection considerations

4.65 Where we exercise this power, it is possible that the information we seek to remotely view may include personal data. Consistent with paragraph 3.54 above, we will seek to limit the personal data which we remotely view to that which is necessary for the performance of our functions. We will discuss with the recipient of our information notice what personal data (if any) we consider relevant for the purpose our functions, and practical arrangements to ensure that, to the extent possible, we are not viewing personal data that is unlikely to be relevant. Services may find it helpful to refer to relevant ICO guidance, including ICO's "A Guide to Lawful Basis" and "A Guide to Data Security".

[76] The Explanatory Notes to the Online Safety Act 2023 state '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'.

Receiving a Remote Viewing Information Notice

4.66 We are required to give the recipient at least seven calendar days' notice before they are required to take steps to enable Ofcom to remotely view information in real time.[77]

4.67 We may contact the recipient in advance of sending a Remote Viewing Information Notice to discuss the information that Ofcom may wish to remotely view as well as the technical capabilities in place to support this. Our decision to engage with the recipient at this stage in the process will depend on the complexity of the case.

4.68 In line with our general process for issuing information notices, we would expect to send a draft of the Remote Viewing Information Notice[78] to:

a) provide the recipient with an opportunity to comment on the technical aspects of the steps required to remotely view the real time information;
b) discuss any other information that would be necessary for the purpose of Ofcom remotely viewing the real time information, including the parameters of any demonstration or test; and
c) confirm the time and date for Ofcom's remote viewing of the real time information.

4.69 We will work with services to ensure that the technical parameters for any demonstration or test are clearly understood and that they can provide the required information accurately and in a suitable format.

Responding to the information notice

4.70 The recipient of a Remote Viewing Information Notice should take the steps set out in paragraph 4.31 upon receipt of the notice. In addition, the recipient should also:

a) carefully read the technical parameters for the test or demonstration and ensure what is being requested is understood;
b) contact Ofcom as soon as possible if any aspects are not clear;
c) note the date for providing any additional information following the test or demonstration (in cases where further analysis may be required);
d) confirm the relevant systems and processes are in place to allow Ofcom to remotely view the specified information; and
e) confirm the relevant systems and processes are in place to generate the requested information.

4.71 Where Ofcom issues a Remote Viewing Information Notice, it is likely that the information notice will require the person to provide the results or output of that test or demonstration in writing to ensure that Ofcom has a proper record. The recipient should also take the steps set out at paragraph 4.32-4.33 above.

[77] Section 102(5) of the Act.
[78] Paragraph 4.26 above sets out some examples of time when it is likely to be appropriate to issue an information notice without issuing a draft first.

Specific considerations for Data Preservation Notices under section 101(C1)

Circumstances in which Ofcom has a duty to issue a Data Preservation Notice

4.72 Ofcom is required to issue a Data Retention Notice to a provider of a regulated service in certain circumstances. Those circumstances are when a coroner has:[79]

a) notified us that they are conducting an investigation into the death of a child; and
b) provided us with the following information:

i) the name of the child who has died,
ii) the child's date of birth,
iii) any email addresses which were used by the child (so far as the coroner knows), and
iv) the name of any regulated service which has been brought to the coroner's attention as being of interest in connection to the child's death.

4.73 In addition to the information required in the paragraph above, coroners may wish to provide the following optional information, which may make it easier for service providers to locate a child's account.[80] These are:

a) any known mobile numbers; and,
b) any known usernames or similar.

Persons to whom Ofcom must issue a Data Preservation Notice

4.74 Where a coroner provides us with the information set out at paragraph 4.72 above, we must issue a Data Preservation Notice to:[81]

a) a regulated service that the coroner has notified us is of interest in connection with the child's death, or
b) a regulated service of a kind described in any regulations made by the Secretary of State.[82]

Ofcom's power to issue a Data Preservation Notice

4.75 In addition, where a coroner provides us with the information set out at paragraph 4.72, we also have a power to issue a Data Preservation Notice to certain other people who may hold information relating to the child's use of a regulated service.[83] Those people are the provider of an ancillary service or an access facility in relation to a regulated service, or a person who was the provider of a regulated service, ancillary service or access facility in the past.[84] For example, an access facility may be an app

[79] Section 101(A1), (B1) and (C1)(a) of the Act.
[80] [Reference to relevant part of Chief coroners' guidance when published]
[81] Section 101(C1)(a) and (E1) of the Act.
[82] At present, no such regulations have been made.
[83] Section 101(C1)(b) of the Act.
[84] Section 101(C1)(b) confers this power in relation to "any other relevant person" i.e. any relevant person other than the provider of a regulated service mentioned in sub-paragraph (a). The definition of "relevant person" is set out in section 101(7) of the Act and directs to section 100(5)(a)-(e).

store through which a mobile app for a regulated service used by the deceased child was downloaded.[85]

Obligations imposed by a Data Preservation Notice

4.76 A Data Preservation Notice requires the recipient to ensure the retention of certain information relating to the use of a service by the child who has died. This includes taking all reasonable steps, without delay, to prevent the deletion of such information by the routine operation of systems or processes.[86]

4.77 The information that Ofcom can require the recipient to retain is limited to:

a) information that we have the power to later request under a Coroner Information Notice i.e. information about the use of a regulated service by the child whose death is under investigation.[87] This includes content encountered by the child by means of the service, how the content came to be encountered by the child, how the child interacted with the content, and content generated, uploaded or shared by the child (see paragraphs 4.80 to 4.81 below); or
b) information that the recipient might need to retain to enable them to provide such information in response to a Coroner Information Notice (if one was given in the future).[88]

4.78 We must specify or describe the information to be retained in the Data Preservation Notice.[89] We must also specify why we require the information to be retained.[90]

4.79 In general, we will require regulated services (or persons who were previously regulated services) to retain the following standard set of information.

4.80 For **user-to user services**, we will generally require the retention of the following information:

~~a)~~ content[91] (including direct messages, comments, reactions, etc.) that the child user either uploaded, generated or shared on the service, or encountered[92] by means of the service; and
b) metadata[93] associated with that content, e.g. time, date, account details of a user who uploaded, generated or shared content encountered by the child; how long a child paused on content; etc; and

[85] See section 146(11) of the Act.
[86] Section 101(D1) of the Act.
[87] Section 101(F1)(a) of the Act, referring to information of a kind which Ofcom have power to require under a notice under section 100(1) (and in particular, subsections 2(a)-(d)).
[88] Section 101(F1)(b) of the Act.
[89] Section 102(5A)(a) of the Act.
[90] Section 102(5A)(b) of the Act.
[91] Section 236 of the Act defines "content" to mean "*anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description.*"
[92] Section 236 of the Act defines "encounter" as meaning to *"read, view, hear or otherwise experience content."*
[93] Metadata is a set of descriptive information that describes and gives information about the content which can include various attributes that provide context, structure, and insights into the content, such as type (for example, text, image, video), caption, hashtags, mentions, and engagement (for example, likes, shares, and view counts).

c) any search requests entered by the child to locate content on the service (and metadata associated with those requests e.g. date/time).
d) friend/connection lists and channels that the child followed.[94]

4.81 For **search services**, we will generally require the retention of the following information:

a) search requests entered by the child;
b) the content shown to the child in response to each search request**.** This includes the search results shown to the user on the pages of results that they visited, and any images, warnings, supportive messaging or AI-generated content shown to the user; and
c) metadata associated with the above e.g. the time and date of each search request, details of each search result that the user clicked on.

4.82 Depending on the individual circumstances of a case, we may require the retention of different information to that set out above. We may do this where, for example, the coroner informs us that they would like us to require the retention of different information.

4.83 A Data Preservation Notice must contain information about the consequences of not complying with the notice.[95]

4.84 A Data Preservation Notice must require the information to be retained for one year.[96] We may, in response to information provided by the coroner, extend this period by up to six months at a time.[97] We will do this giving the recipient a further notice varying the original Data Preservation Notice and stating the further period for which information must be retained and the reason for the extension.[98] We may extend the Data Preservation Notice any number of times.[99]

4.85 We can issue Data Preservation Notices at any point during a coroner's investigation into the death of a child. This means that if further information comes to light, the coroner can request that we issue further Data Preservation Notices to additional services.

Responding to the notice

4.86 If we issue a Data Preservation Notice, and the child named in the notice used the service in question, the recipient must, by the deadline specified in the notice, notify us of the steps it has taken to ensure the retention of the information described within the notice.[100] Where the child named in the notice did not use the service, or the recipient does not hold any information of the kind required to be retained, the recipient must notify us of this fact by the deadline.[101] In either case, we must share

[94] See paragraph 3.18 of the consultation.
[95] Section 102(5A)(e) of the Act.
[96] Section 102(5A)(c) of the Act.
[97] Section 102(5B) of the Act.
[98] Section 102(5C)(a) of the Act.
[99] Section 102(5C)(b) of the Act.
[100] Section 102(5A)(d)(i) of the Act.
[101] Section 102(5A)(d)(ii) of the Act.

this information with the coroner[102] and will do so without further notifying the provider of the information.

Cancelling a Data Preservation Notice

4.87 If the coroner informs us that they no longer require the information to be retained, we must cancel the Data Preservation Notice and will notify the recipient of this.[103]

Specific considerations for Coroner Information Notices under section 101(1)

Overview of Ofcom's power to issue a Coroner Information Notice in response to a coroner's request

4.88 Coroners have existing powers to require information for the purpose of their functions. Under those powers, a coroner may request information from Ofcom for the purposes of an investigation or inquest into the death of a child.[104]

4.89 In that event, we have discretion to issue a Coroner Information Notice under section 101(1) of the Act for the purpose of responding to the coroner's request. Ofcom may also issue a Coroner Information Notice for the purpose of preparing a report under section 163 in connection with an investigation or inquest into the death of a child.

4.90 We may only issue a Coroner Information Notice to providers of regulated services, providers of ancillary services or access facilities, or a person who was a provider of a regulated service or a provider of an ancillary service or access facility at the time to which the required information relates.[105]

4.91 Where we decide to issue a Coroner Information Notice, we can require information about the use of a regulated service by the child whose death is under investigation, including, in particular:

a) content encountered by the child by means of the service;
b) how the content came to be encountered by the child, including the role of algorithms or particular functionalities of a service;
c) information about how the child interacted with the content, for example by viewing, sharing, storing, pausing on or enlarging it; and
d) content generated, uploaded or shared by the child.

4.92 As with information notices issued under section 100 (see paragraph 4.14 above), Coroner Information Notices may require the production of documents held outside the UK.[106]

4.93 Our typical process explained from paragraph 4.25 will also apply when we issue a Coroner Information Notice under section 101(1). Where a recipient provides

[102] Section 101(G1) of the Act.
[103] Section 102(9A) of the Act.
[104] Paragraph 1(2) of Schedule 5, Coroners and Justice Act 2009; section 17A(2) of the Coroners Act (Northern Ireland) 1959 (c. 15 (N.I.)). In Scotland, a procurator fiscal's power to issue Ofcom an information requests comes from common law to investigate deaths.
[105] Section 101(7) of the Act.
[106] Section 204(2) of the Act.

comments in response to a draft Coroner Information Notice, we will generally disclose these comments to the coroner without further notification to the service.[107] The draft notice will inform the recipient that we intend to take this approach.

Coroners' requests to Ofcom and Ofcom's discretion to issue a Coroner Information Notice

4.94 Ofcom has discretion to issue a Coroner Information Notice for the purpose of responding to a request from a coroner.

4.95 The Chief Coroner in England and Wales has issued guidance to coroners on obtaining of information regarding a child's social media use in connection with Ofcom's powers under section 101 of the Act.[108] In line with that guidance, where a coroner requests information from Ofcom in connection with the death of a child, we would ordinarily expect that the request would:

a) identify the child whose death is the subject of the investigation or inquest;
b) identify a particular service or various services of interest (this is particularly important as it may not be feasible for Ofcom to issue a Coroner Information Notice unless Ofcom can understand the relevant services in question);
c) describe the information sought. In doing so, we would encourage coroners to consider:
    i) whether they are seeking **content**[109] and, if so:
    ii) what was the child's **relationship to the content**? I.e. is it content that the child uploaded, generated or shared? Or content that the child encountered[110]? Or both?
    iii) what **type of content** is sought? I.e. is it all content types or specific kinds? For example, direct messages, likes, comments or reactions etc.
    iv) are they seeking **content** associated with search? If so, are they interested in the search requests entered by the child (this could be on a user-to-user service where this has a search functionality, and/or a search service), the content shown in response to a search request, or both? If they are seeking content shown in response to a search request, should this include AI-generated content shown to the child?
    v) whether they are seeking **metadata**[111] related to that content (e.g. date / time, the account details of another user who generated, uploaded, or shared content which the child encountered, etc.)? Or are they seeking other metadata not associated with content (e.g. date / time an account was created)?
d) describe the timeframe within which the information is sought; and
e) set a reasonable deadline for Ofcom to respond, which takes into account the time it will take Ofcom to issue its Coroner Information Notice and obtain the relevant information.

4.96 When identifying the child whose death is the subject of the investigation or inquest, we would expect coroners to provide Ofcom with any usernames and/or contact

[107] Ofcom may disclose information with respect to a business which has been obtained in the exercise of Ofcom's statutory powers for the purpose of facilitating the carrying out by a coroner of its statutory functions in connection with inquests and investigations: section 393 of the Communications Act, in particular sub-sections (2)(b), (3)(ha)-(hb), (4) and (5)(ca), (nb) and (s).
[108] Guidance No 46 Obtaining information regarding social media use - Courts and Tribunals Judiciary.
[109] See footnote [91].
[110] See footnote [92].
[111] See footnote [93].

details known to have been used by the child. When describing the timeframe within which the information is sought, we would encourage coroners to consider how to narrow the timeframe to that which is necessary and relevant in the context of the investigation or inquest. This is more likely to ensure that it is feasible for recipients to respond by the proposed deadline and will reduce the risk that coroners have to deal with voluminous irrelevant information.

4.97 Where a coroner's request follows the approach set out above, it will facilitate Ofcom in deciding whether to issue a Coroner Information Notice; in particular, it will enable us to better assess if such a notice would be a feasible and proportionate way to obtain the information requested.

4.98 We will consider each coroner's request on a case-by-case basis, taking into account all relevant factors (including the extent to which the coroner's request has provided the above information) before deciding whether it is proportionate to issue a Coroner Information Notice for the purpose of our response. In the first instance, we expect to engage with the coroner informally before they request information from us. In general, this will involve Ofcom meeting with the coroner to discuss the scope and details of the request. The purpose of this engagement is to understand the coroner's requirements in a particular case, to discuss the reasonableness of the proposed request, and to seek to agree on the parameters of each individual request. As part of these discussions, we may also support the coroner to explore potential alternative ways of obtaining the information sought; for example, where services may have a policy of disclosing information directly to parents of deceased children.

4.99 We expect that this close engagement and communication between Ofcom and the coroner will continue over the lifecycle of a case.

4.100 Coroners who wish to discuss a potential request with us should contact CoronersSupport@ofcom.org.uk. We will aim to acknowledge any requests within 48 hours of receipt.

Data protection considerations in relation to Coroner Information Notices

4.101 A Coroner Information Notice may, in principle, require the provision of personal data. This is because such notices may require (among other things) content encountered by the child by means of the service, and content generated, uploaded or shared by the child. Although information relating to a deceased person does not constitute personal data and is therefore not subject to the UK GDPR, the information sought may, depending on the case, include the personal data of other users. We will endeavour to engage with coroners to understand the extent to which they require personal data for the purpose of their functions and ensure that any Coroner Information Notice is not likely to require the disclosure of more personal data than needed to fulfil the purposes of the request.

Responding to a Coroner Information Notice and disclosure of information obtained under a Coroner Information Notice

4.102 In accordance with the approach set out in section 3, we will generally specify in a Coroner Information Notice that, if the recipient considers that any information provided in response is confidential, the recipient should identify that information and explain why it is confidential. Further, as noted above, we will, to the extent possible,

take account of any legislation which may restrict the ability of a recipient of a notice to provide certain information to us. However, it will be the responsibility of the recipient to draw any such legislation to our attention and to explain how it restricts their ability to respond.

4.103 Where we decide to issue a Coroner Information Notice, we will generally disclose information provided in response to the notice (including information claimed to be confidential) to the requesting coroner without further notification to the recipient of the notice.[112] The notice will inform the recipient that we intend to take this approach.

4.104 Where the recipient has claimed that information in its response is confidential, and explained why, we will pass on this explanation to the coroner. We would generally expect the recipient of a Coroner Information Notice and the coroner to liaise between themselves regarding the confidentiality of any information that Ofcom disclosed for the purpose of responding to the coroner's request.[113] We generally will not review or analyse the information provided, except to ensure it is complete.

Naming a senior manager

4.105 Where we send an information notice under section 100 or 101 to a regulated service provider, and that provider is an entity, we may require it to name a relevant senior manager who may reasonably be expected to be in a position to ensure compliance with the notice.[114]

4.106 A senior manager is an individual who plays a significant role in making decisions about or managing and organising the service's activities that relate to the subject matter of the information notice.[115] The senior manager named must be an individual and so cannot be a team of individuals.

4.107 The senior manager named is expected to ensure compliance with the requirements of the notice. This includes ensuring the response to the information notice is complete, accurate, in the format and manner required by Ofcom, and the information requested is provided by the deadline set.

4.108 We will decide on a case-by-case basis whether to include this requirement, having considered whether it is necessary and proportionate to do so. We will take into consideration the entity's history of compliance and co-operation with Ofcom, including its history of compliance with any previous requests for information, where appropriate, as well as the burden this requirement would place on the entity and the named senior manager.

4.109 We note that we may take enforcement action against a regulated service provider in relation to its compliance with an information notice (see Section 8 for further details). Where we take such enforcement action in circumstances where the information

[112] Ofcom may disclose information with respect to a business which has been obtained in the exercise of Ofcom's statutory powers for the purpose of facilitating the carrying out by a coroner of its statutory functions in connection with inquests and investigations: section 393 of the Communications Act, in particular sub-sections (2)(b), (3)(ha)-(hb), (4) and (5)(ca), (nb) and (s).
[113] It is ultimately for the coroner to decide which documents may need to be disclosed to interested persons and to ensure that any necessary redactions are made.
[114] Section 103(1)-(2) of the Act.
[115] Section 103(4) and (5) of the Act.

notice included a requirement to name a senior manager, in most cases we do not expect to publish the name of the senior manager as part of that enforcement action.

4.110 An entity commits an offence if it fails to comply with an information notice (for example by not providing clear, complete and accurate responses to all the questions by the deadline given).[116] If the named senior manager fails to take all reasonable steps to prevent that offence being committed, they will also have committed an offence.[117] In addition, if an entity commits an offence by:

a) knowingly or recklessly providing information that is false in a material respect in response to the information notice;[118]
b) intentionally providing an encrypted document or information in response to an information notice such that it is not possible for Ofcom to understand it;[119]
c) intentionally preventing the information from being provided by suppressing, destroying or altering the information or document (or causing or permitting this to happen);[120] or
d) intentionally deletes or alters, or causes or permits the deletion or alteration of, information required to be retained pursuant to a Data Preservation Notice.[121]

4.111 If the senior manager failed to take all reasonable steps to prevent any of those offences being committed, then that senior manager will have committed an offence.[122]

4.112 More information about the consequences for non-compliance can be found in Section 8, including information about defences that may be available to named senior managers in the event they are prosecuted for a criminal offence.

4.113 If we decide to bring criminal proceedings against a named senior manager their name would normally be a matter of public record.

4.114 If we impose a requirement to name a senior manager within the information notice, we will also require the service to inform the named senior manager.[123] We will normally ask the service to provide evidence that the senior manager has been provided with the information notice and has acknowledged that they have been named as a senior manager.[124] We will also include information about the consequences for the named individual, should the service fail to comply with the requirements within the information notice.[125]

---

[116] See section 109(1) of the Act; and further Section 8 below.
[117] Section 110(2) of the Act. See further Section 8 below.
[118] Such that the entity commits an offence under section 109(3) of the Act; see further Section 8 below.
[119] Such that the entity commits an offence under section 109(4) of the Act; see further Section 8 below.
[120] Such that the entity commits an offence under section 109(5) of the Act; see further Section 8 below.
[121] Such that the entity commits an offence under section 109(6A) of the Act; see further Section 8 below.
[122] Sections 110(4), (5), (6) and (6A) of the Act. See further Section 8 below.
[123] Section 103(3)(a) of the Act.
[124] We note that, where a senior manager is charged with an offence pursuant to section 110 of the Act, it is a defence to show that they had no knowledge of being named as a senior manager in a response to the information notice in question: section 110(8).
[125] Section 103(3)(b) of the Act.

5. Reports by a skilled person under section 104

Introduction

5.1 Section 104 of the Act grants us the power to appoint a skilled person, or to require the provider of a service to appoint a skilled person, to provide a report ('a skilled person's report') in certain circumstances set out below. A skilled person is a person appearing to Ofcom to have the skills necessary to prepare a report about matters that Ofcom considers to be relevant. A skilled person will be appointed by Ofcom or nominated and approved by Ofcom but appointed by the provider.[126]

5.2 This section will set out when we may use this power and the process we will typically follow.

When Ofcom might require a skilled person's report

5.3 We may appoint a skilled person where we consider it necessary to:

a) assist us to identify and assess a service's failure (or possible failure) to comply with a 'relevant requirement';[127] or
b) develop our understanding of the nature and level of risk of such a compliance failure, and ways to mitigate that risk.[128]

5.4 Additionally, we are required to appoint a skilled person to prepare a report before deciding whether to issue a notice to deal with terrorism content or child sexual exploitation and abuse ('CSEA') content (or both) under section 121(1) of the Act.[129]

5.5 A skilled person is a person appearing to Ofcom to have the skills necessary to prepare a report about matters that Ofcom considers to be relevant.99 A skilled person could be an individual, a firm or an organisation. We are only likely to consider that a person has the skills necessary to prepare a report about relevant matters where that person is independent from the service or service provider or can otherwise demonstrate that no potential conflict of interest could arise. We are also only likely to appoint a skilled person where we are satisfied that the person has appropriate safeguards in place to ensure confidential information is not disclosed to anyone other than Ofcom.

5.6 In line with the approach set out in section 3, we will exercise our power to appoint a skilled person, or to require the provider of a service to appoint a skilled person, in a proportionate manner. Section 3 sets out factors we will generally take into account when making this assessment.

5.7 The following are examples of when we may consider it necessary to exercise our power to obtain a skilled person's report:

[126] Section 104(6) of the Act.
[127] 'Relevant requirement' is defined in section 104(13) of the Act.
[128] Section 104(1) of the Act; see also section 104(2).
[129] Sections 104(3) and 122(1) of the Act.

a) where we have concerns that require independent external, expert analysis, in order to determine the nature and severity of the issues at hand;
b) where we consider a service provider is unable to provide the information we require, for example due to the level of co-operation they have demonstrated, or the specific or technical nature of the information needed; or
c) where the subject matter is technically complex and requires specialist resources or skills that Ofcom may not have in-house.

5.8 Where we have compliance concerns, we may use a skilled person's report to understand the measures that a service provider could put in place to become compliant. To understand what measures could be put in place, the skilled persons report may include:

a) an assessment of **compliance risks** where we believe that a service is at risk of failing to comply with any relevant requirement and gathering information to inform us on the nature of that risk;
b) **monitoring identified risks** and understanding any measures a service has taken to reduce or mitigate the risk; and
c) understanding how to **prevent, limit or reduce the identified risk**(s) from crystallising or increasing.

5.9 In general, we do not expect to use our skilled persons reports as often as our section 100 information notices power, and these will typically be reserved for more serious or complex cases.

Typical process

5.10 We would typically engage with the service before exercising our power to require a skilled person's report. This could be, for example, to help us decide whether to exercise this power, to understand what information the service may have, or to decide on how the appointment process should go ahead.

5.11 Where we decide to exercise our power to require a skilled person's report, we will either:

a) appoint the skilled person ourselves and notify the service of that appointment; or
b) give the service provider a notice requiring it to appoint a skilled person (please see paragraphs 5.15(a) and (b) below for further detail).

5.12 Paragraphs 3.62 – 3.66 above sets out guidance regarding how we will serve notices, including the notices referred to in the paragraph above.

5.13 Whether we appointed a skilled person, or require the provider to appoint a skilled person, we will specify in our notice the matters to be explored in the report.[130]

5.14 We will decide whether to appoint the skilled person, or whether to require the service provider to appoint them, on a case-by-case basis. However, in circumstances where

[130] Section 104(4) and (5).

we are looking to issue a notice to deal with terrorism content or CSEA content (or both) under section 121(1), we must appoint the skilled person.[131]

5.15 Where we give a service provider a notice requiring it to appoint a skilled person, we will either:

a) **Nominate a specific skilled person for the service provider to appoint**. This nomination will typically be included in the notice to appoint a skilled person. In some cases, where we have initially allowed the service provider to select a skilled person for our approval but have ultimately not approved the provider's recommended skilled person, we may nominate a skilled person subsequently in correspondence.

b) **Request that the service provider select a skilled person for our approval**. In this case, we will only approve a skilled person selected by the service provider where we consider that they have the skills necessary to address the matters specified in the notice and there are no conflicts of interest that may affect their ability to give an objective opinion. Where we require a service provider to appoint a skilled person subject to our approval, we will explain what information we expect the service provider to give Ofcom about its selected candidate(s), such as an explanation of the expertise, skills and qualifications of the skilled person. Service providers may take the cost associated with the skilled person report into account when deciding what skilled person to select for our approval.

5.16 We will determine how much communication between Ofcom and the skilled person will be necessary following their appointment. To this end, we will typically request to see a draft report, and may ask for regular updates from the skilled person on their progress.

5.17 The service provider and anyone who works for the service (or who used to work for the service), or who is providing services to the service provider on relevant matters, are under a duty to give the skilled person all such assistance as they may reasonably require to prepare the report.[132] We do not consider that this duty requires those subject to it to provide information subject to legal professional privilege to the skilled person.

5.18 The provider of the service is liable for the payment, directly to the skilled person, of the skilled person's remuneration and expenses relating to the preparation of the report.[133] If the provider of the service fails to make payment, the amount due can be recovered by order of court.[134]

[131] Section 122(1) says we may give a notice under section 121(1) to a provider only after obtaining a report from a skilled person appointed by OFCOM under section 104(1). For further details see our [draft] Technology Notices to deal with terrorism and/or CSEA content: Draft Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023 (16 December 2024).
[132] Section 104(7) of the Act
[133] Section 104(8) of the Act.
[134] Section 104(9)-(12) of the Act.

6. Interviews under section 106

Introduction

6.1 Ofcom may open an investigation into whether a provider of a regulated service has failed, or is failing to comply with a requirement imposed by any enforceable requirement as set out in section 131 of the Act or to comply with a notice to deal with terrorism and CSEA content.[135] Once we have opened an investigation, we may require an individual to attend an interview to answer questions and provide explanations on any matter relevant to the investigation by issuing a notice under section 106 of the Act.[136]

6.2 In this section, we explain when we might exercise our power to require interviews, and the typical process we will follow.

6.3 An individual who fails to comply with the exercise of Ofcom's power to require an interview may have committed a criminal offence; see Table 8.1 for details.

When Ofcom might require attendance at an interview

6.4 Where we have opened an investigation, we will decide on a case-by-case basis whether to require a person to attend an interview. We may do so where, for example:

a) we believe, based on the evidence available at the time, that gathering information from an individual (including senior management) may help us identify the root cause of the compliance failure;
b) it would be beneficial to obtain first-hand accounts and individual experiences in relation to a potential failure; or
c) there are no or limited records that can be gathered by other means.

6.5 The Act specifies the classes of individuals that we can require to attend an interview. These are:

a) if the service provider is an individual or individuals, those individual(s);
b) an officer of the provider of the service;
c) where the service provider is a partnership, a partner;
d) an employee of the provider of a service;
e) a person who has previously held a position within (a)-(d) at the time the required information or explanation relates to.[137]

6.6 We can require such an individual to attend an interview even if they are outside the UK.[138]

6.7 If Ofcom requires an individual to attend an interview, that individual is not required to disclose legally privileged information to Ofcom.[139]

[135] Section 105 of the Act.
[136] Section 106 of the Act.
[137] Section 106(4) of the Act.
[138] Section 204(3) of the Act.
[139] Section 106(6) of the Act.

6.8 If an individual required by Ofcom to attend an interview fails to attend and answer questions, they may have committed a criminal offence. See Table 8.1 for more information.

Typical process

6.9 We will give the individual concerned a notice requiring them to attend at a specified time and place, and to answer questions and provide explanations about any relevant matter.[140] The notice will set out the subject matter and purpose of the interview and contain information about the consequences of non-compliance.[141]

6.10 Paragraphs 3.62 - 3.66 above set out guidance regarding how we will serve notices, including a notice requiring an interview. We note that, where we send a notice to an individual who is not the provider of a regulated service, we may send the notice to their home address or, if they are currently connected with a provider of a regulated service, the address of the provider's registered or principal office. [142]

6.11 If we require an officer or employee of a service provider, or a partner in a service provider (if they are a partnership) to attend an interview, we will provide the relevant service provider with a copy of the notice given to that individual.[143]

6.12 Prior to issuing the notice, we may issue a draft notice or engage with the individual or service provider by other means to inform them that we intend to use our interview power and make advance arrangements for the time and location of the interview, which will be confirmed in the notice. This may not always be possible or appropriate depending on the nature and circumstances of the investigation at hand.

6.13 When the final notice is issued, we will allow a reasonable time period between issuing the notice and conducting the interview, taking into account all relevant factors. Typically, this will be at least seven calendar days, unless there is urgency in the matter.

6.14 Further to issuing the notice, we expect the individual to acknowledge receipt and confirm that they are able to attend the interview at the time and place specified in the notice.

6.15 In exceptional circumstances and where we have received notice as far in advance as possible, we may agree to a request to rearrange the interview. We would expect the individual or their legal representatives to contact us as soon as possible if they are at risk of not being able to comply with the notice and not being able to attend the interview.

6.16 We may decide that it is appropriate to conduct the interview virtually. In making this decision we will take account of all relevant factors, which may include the geographical location of the individual and the cost and time required for them to attend in person (for example, if the individual is outside of the UK and it would be

[140] Section 106(2) of the Act.
[141] Section 106(3) of the Act.
[142] Section 208(9) of the Act.
[143] Section 106(5) of the Act.

costly or be otherwise onerous to attend in person). We will also consider any other reasonable adjustments that need to be made.

6.17 If the individual has requested it, they may be accompanied by a legal adviser when answering our questions. If their legal adviser is unavailable on the date specified in the notice, we are likely to delay the interview by a reasonable period so as to allow the legal adviser to attend. We will decide this on a case-by-case basis. Reasonable breaks in the interview can be requested to allow time for the person to talk with their legal adviser.

6.18 Should any party involved in the interview require a copy of minutes or transcripts, this should be agreed by all at the outset of the interview and arranged on a case-by-case basis.

6.19 Ofcom will not reimburse any of the costs incurred by the individual being interviewed or the service provider relating to Ofcom's decision to exercise its interview power, including for example, the cost of obtaining legal advice, or travel costs.

7. Powers of audit, entry and inspection under Schedule 12

Introduction

7.1 Schedule 12 to the Act grants Ofcom the power to authorise persons to:

a) enter and inspect certain premises without a warrant;[144]
b) apply for and execute a warrant to enter and inspect certain premises;[145] and/or
c) carry out audits on a service (which may also involve entering and inspecting premises).[146]

7.2 In general, our use of powers of entry, inspection and audit will typically be reserved for more serious or complex cases. The threshold for using these powers is high because we recognise that entering and inspecting premises (including as part of an audit) is a significant step and is one we do not anticipate taking often. We are only likely to enter and inspect premises where our other information gathering powers are unlikely to enable us to obtain the information we need to perform one or more of our regulatory functions under the Act.[147]

7.3 We can only exercise our powers of entry and inspection (both with and without a warrant) on premises used by the provider of a regulated service in connection with the provision of that service.[148] We cannot exercise these powers, or our audit power, in relation to domestic premises.[149] We also cannot exercise these powers to require the disclosure of information or documents which are legally privileged.[150]

7.4 Only specific staff authorised in writing by a sufficiently senior person with delegated authority from Ofcom's Board will be able to authorise persons to exercise the powers outlined in this section.[151] See Section 3 of this Guidance for detailed information on Ofcom's general duties when exercising information gathering powers; including proportionality, confidentiality, disclosure of information, record retention and personal data, information security, and privileged information.

7.5 The consequences of a failure to comply with the powers set out in this section could include:

a) enforcement action by Ofcom; or
b) criminal liability.

---

[144] Paragraphs 2-3 of Schedule 12 to the Act.
[145] Paragraphs 5-15 of Schedule 12 to the Act. A warrant is a legal document issued by the court that grants us certain powers specified within it.
[146] Paragraph 4 of Schedule 12 to the Act.
[147] See section '*We will exercise our powers in a proportionate way*' above from paragraph 3.10 for more information.
[148] Paragraphs 2(1)(a) and 5(1)(a) of Schedule 12 to the Act.
[149] Paragraphs 4(4), 17(2) and 19 of Schedule 12 to the Act. Domestic premises are defined in the Act as premises, or a part of premises, used as a dwelling.
[150] Paragraphs 4(5) and 17(3) of Schedule 12 to the Act.
[151] See paragraph 1 of Schedule 12 to the Act.

7.6 Section 8 of this Guidance sets out the consequences of non-compliance with our audit, entry and inspection powers in more detail.

Home Office code of practice on powers of entry

7.7 When we are entering and inspecting premises without a warrant, executing a warrant to enter and inspect premises, or where we are exercising our audit power to require a provider to enable us to enter and inspect premises, we must follow the requirements set out in the Act, and must also take into account the Home Office's code of practice on powers of entry (the 'Code') where relevant.

7.8 The Code is relevant where the Act is silent on particular matters.[152] By way of illustration, the Act does not define what a 'reasonable hour' for entry is, but the Code says this should be determined by reference to the normal working practices of the particular business concerned. In those circumstances we will have regard to the Code's definition of 'reasonable hour'. This Guidance is intended to supplement the Code: for example, the Code does not address whether the person exercising entry and inspection powers should allow the occupier's legal advisers to be present during an inspection; however, we have set out below that service providers are entitled to have legal advisers present. In the event of any unintentional inconsistency between this Guidance and the Code, this Guidance shall take precedence.

7.9 It is important to note that the Code does not take precedence over the requirements of the Act. As such, an authorised person exercising powers of entry *must adhere* to the requirements of the Act while *having regard to* the Code, as supplemented by this Guidance.

7.10 The remainder of this section constitutes our proposed approach to using our powers of audit, entry and inspection under Schedule 12 to the Act. We have drafted it to be consistent with the Code, apart from where we have good reason to take a different approach or where the legislation requires us to do so.

Entry and inspection without a warrant

When Ofcom might exercise this power

7.11 We may use our powers of entry and inspection without a warrant in connection with the exercise of any of our regulatory functions under the Act.[153] However, we may only exercise these powers so far as is required in connection with those functions, and not further.[154]

7.12 Circumstances in which we might use this power include, but are not limited to, where a service may have failed to comply with an enforceable requirement and we believe there is information or equipment on the premises relevant to our investigation into that suspected failure.

[152] The Code, paragraph 5.1.
[153] Paragraph 2(7) of Schedule 12 to the Act.
[154] Paragraph 2(7) of Schedule 12 to the Act.

Typical process

Receiving a notice of entry and inspection without a warrant

7.13 If we are going to enter and inspect premises that we believe are used by the provider of a regulated service in connection with the provision of the regulated service, we must give the occupier[155] of the premises (in practice, this is likely to be the service provider) at least seven calendar days' written notice (we will refer to this written notice as an '**Entry and Inspection Notice**').[156]

7.14 The Entry and Inspection Notice will include details of the following:

a) the date, time and purpose of the proposed entry;[157]
b) that the entry will be conducted without a warrant;
c) the powers we will be exercising;
d) the occupier's rights;
e) any compensation or complaints procedures that exist; and
f) where a copy of the Code may be obtained.[158]

7.15 If we are to require the occupier to provide us with information, documents or a test or demonstration during the inspection, the Entry and Inspection Notice will also set out:

a) any information that they must provide;
b) any documents that they must produce;
c) any test or demonstration that they must perform during the inspection;[159] and
d) the consequences of not complying with the requirements outlined in the notice.

7.16 From paragraphs 3.62 we above set out guidance regarding how we will serve all notices, including the Entry and Inspection Notice.

On the day of the inspection

7.17 We may only exercise this power at a reasonable hour.[160] We will determine what constitutes a 'reasonable hour' by reference to the normal working practices of the particular business concerned.[161]

7.18 When we attend the premises, the authorised person leading our inspection will, if asked to do so, show the occupier evidence of their identity, the Entry and Inspection Notice and their authorisation to exercise the power of entry and inspection. They will also explain why we require access to the premises and the length of time the inspection is likely to take.[162]

7.19 More than one authorised person may attend the premises on the day of inspection; the number of authorised persons we bring will be reasonable and proportionate in

---

[155] The Code defines 'occupier' as a person who is or appears to be in charge of the premises: paragraph 4.8.
[156] Paragraph 2(1)(b) of Schedule 12 to the Act.
[157] The Code, paragraph 8.2.
[158] The Code, paragraph 7.3.
[159] Where we require the occupier to perform a test or demonstration during an inspection, paragraphs 4.41-4.50 above will apply.
[160] Paragraph 2(2) of Schedule 12 to the Act.
[161] The Code, paragraph 13.1.
[162] Paragraph 2(3) of Schedule 12 to the Act.

enabling us to exercise our power of entry and inspection without a warrant effectively.[163]

7.20 The occupier may have legal advisers present at the premises throughout our inspection. Given that we will provide seven calendar days' notice of our intention to enter and inspect premises without a warrant, we would expect any legal advisers who plan to attend to be present on our arrival. If they are not present, we will not wait for them to arrive before commencing our entry and inspection.

7.21 The specific actions we will take during an inspection will depend on the individual circumstances in that case, but the actions we are authorised to take are as follows:[164]

a) enter the premises;
b) inspect the premises;
c) observe the carrying on of the service – including viewing, using equipment or a device on the premises, information generated in real time by the performance of a test or demonstration that we have specified in our Entry and Inspection Notice;[165]
d) inspect any document or equipment found on the premises;
e) require any person who is on the premises to provide any information or produce any document that we think is relevant to the provision of the service; and
f) require any person on the premises to provide an explanation of any document or to tell us where we can find it.

7.22 We can also take copies of any document found or produced while we are exercising the powers outlined in paragraph 7.21 (a)-(f) above.[166]

7.23 During our inspection we will expect occupiers to give reasonable assistance to the authorised persons exercising our Schedule 12 powers. That might include things like unlocking doors and opening containers.[167]

7.24 It is important to note that it is an offence for an occupier of a premises to intentionally obstruct or fail to comply with a requirement made under Schedule 12.[168] See Section 8 of this Guidance for full details of the consequences of a failure to comply with requirements made under Schedule 12.

Entry and inspection with a warrant

When Ofcom might exercise this power

7.25 In certain circumstances a person authorised by Ofcom may apply to a justice of the peace or, in Northern Ireland, a lay magistrate for the issue of a warrant to enter and inspect premises.[169]

[163] The Code, paragraph 9.1.
[164] Paragraph 2(4)(a)-(f) of Schedule 12 to the Act.
[165] As noted above, where we require the occupier to perform a test or demonstration during an inspection, paragraphs 4.41-4.50 above will apply.
[166] Paragraph 2(6) of Schedule 12 to the Act.
[167] The Code, paragraph 18.1.
[168] Paragraph 18(1) of Schedule 12 to the Act.
[169] Paragraph 5 of Schedule 12 to the Act.

7.26 In order to apply for a warrant under this paragraph of Schedule 12 to the Act we will need to satisfy the justice of the peace or lay magistrate that:

a) the premises we plan to enter are being used by the provider of a regulated service in connection with the provision of that service (and are not domestic premises);[170]
b) there are reasonable grounds to suspect that the provider is failing or has failed to comply with an enforceable requirement;[171]
c) there is information or equipment on the premises, or documents on the premises, which are relevant to our investigation of that suspected failure; and
d) one of the following conditions also applies:[172]

   i) we have issued an Entry and Inspection Notice (as described above) but were denied entry to the premises when we attended;
   ii) a requirement we imposed while exercising our powers of entry and inspection without a warrant was not complied with;
   iii) a requirement we set out in an Entry and Inspection Notice has not been complied with;
   iv) a requirement set out in an audit notice has not been complied with;
   v) giving notice that we will enter the premises would defeat the object of entry; for example, where we are concerned that information relevant to our investigation may be destroyed or interfered with if notice was given; or
   vi) we need to access to the premises urgently.

7.27 We are not required to give prior notice before executing a warrant and will not typically do so.

7.28 Once a warrant has been issued, we must execute it within one month.[173] A warrant authorises us to enter premises on one occasion only, unless it specifies that it authorises multiple entries.[174]

Typical process

Before we enter

7.29 We will only exercise this power at a reasonable hour,[175] unless it appears that the purpose of the search would be frustrated or seriously prejudiced by entering at a reasonable hour.[176]

7.30 As noted above, the occupier may have legal advisers present at the premises throughout our inspection. Since we will not typically provide notice of our intention to enter and inspect with a warrant, in cases where there is no in-house lawyer already on the premises we may wait a reasonable time for legal advisers to arrive.[177] During

[170] Paragraph 5(1)(a) and 17(2) of Schedule 12 to the Act.
[171] Paragraph 21 of Schedule 12 to the Act sets out the definition of 'enforceable requirement' that applies in this context.
[172] Paragraph 5(2) of Schedule 12 to the Act.
[173] Paragraph 10 of Schedule 12 to the Act.
[174] Paragraph 14 of Schedule 12 to the Act.
[175] A reasonable hour will be determined by reference to the normal working practices of the particular business concerned. The Code, paragraph 13.1.
[176] Paragraph 9 of Schedule 12 to the Act.
[177] A "reasonable time" means such period of time as the authorised person considers is reasonable in the circumstances.

this time, authorised persons may take necessary measures to prevent tampering with evidence.[178]

7.31 We will give the occupier, or any other person who is in charge of the premises, a copy of the warrant before we enter.[179]

7.32 If asked to do so, the authorised person in attendance will also produce evidence of their identity and explain why they are exercising this power.[180]

7.33 We may use reasonable force to facilitate us exercising our powers under a warrant if necessary,[181] including in circumstances where no one is present at the premises when we attend.

7.34 If no one is present at the premises when we attend, we will leave a copy of the warrant in a prominent place,[182] and leave the premises as effectively secured against trespassers as it was when we arrived.[183]

Who can attend the premises

7.35 The Act enables the authorised person who is exercising powers under a warrant to take whichever people, equipment and materials onto the premises that they think are necessary.[184] In practice, this would mean that we may bring, for example, a technical or other subject matter expert to the premises to help us to gather the information we need for our investigation.

7.36 A person we bring onto premises for the reasons outlined above can carry out any of the actions listed at paragraph 7.37 below, as long as they are in the company and under the supervision of a person authorised under the warrant.[185]

Actions we can carry out under a warrant

7.37 As with our other Schedule 12 powers, the specific actions we may carry out under each warrant will depend on the circumstances. In summary, we can:

a) enter the premises;
b) search the premises;
c) inspect any documents or equipment found on the premises, or any information capable of being viewed using equipment or a device on the premises;
d) require any person on the premises to provide us with the information we ask for. This includes requiring an explanation of: (i) any document we find on the premises; or (ii) any information capable of being viewed using equipment or a device on the premises;
e) require any person on the premises to produce any document that in their possession or control;

[178] This could include sealing filing cabinets, keeping business records in the same state and place as when authorised persons arrived, suspending external email or the making and receiving of calls, and/or allowing authorised persons to enter and remain in offices of their choosing.
[179] Paragraph 6(1)(a)-(b) of Schedule 12 to the Act.
[180] Paragraph 6(1)(c) of Schedule 12 to the Act.
[181] Paragraph 13 of Schedule 12 to the Act.
[182] Paragraph 6(2) of Schedule 12 to the Act.
[183] Paragraph 15 of Schedule 12 to the Act.
[184] Paragraph 11 of Schedule 12 to the Act.
[185] Paragraph 12 of Schedule 12 to the Act.

f) take copies of any document we find on the premises or which is produced in response to a requirement we make under paragraph e) above;
g) require electronically stored information which can be accessed from the premises to be produced for us: (i) in a form which enables us to take it away, for example as a printout or on a memory stick; and (ii) in which it is visible and legible (or from which it can readily be produced in a visible and legible form);
h) use equipment on the premises to produce electronic information in a different form as required;
i) require any person on the premises to assist us to produce the information we need in a different form, or to operate the equipment needed to do so, or to provide any other assistance that we may reasonably require;
j) take copies of anything produced in accordance with paragraph (g);
k) seize any document or equipment we find on the premises or any document produced in response to a request under paragraph (e), or anything produced in accordance with paragraph (g);
l) open any container we find on the premises; and
m) take a photograph or video recording of anything we find on the premises.[186]

Our powers of seizure

7.38 As noted at paragraph 7.37 above, under a warrant we will also have powers of seizure, which means that we will be able to take away items that will facilitate our investigation, like relevant documents or equipment.[187]

7.39 If asked to do so, the person executing the warrant will provide a receipt for any item we seize and a copy of any document we seize while on the premises, unless this would result in undue delay.[188] We can retain anything we seize under a warrant for as long as we think is necessary.[189]

Audit

When Ofcom might exercise this power

7.40 We may carry out an audit in order to assess whether a provider has complied, or is complying, with enforceable requirements that apply in respect of a service.[190] Alternatively, we may carry out an audit to assess the nature and level of risk of any failure to comply with an enforceable requirement that applies to a service, and ways to mitigate such a risk.[191]

7.41 We may require a provider to pay some, or all, of the reasonable costs of an audit.[192]

[186] Paragraph 7 of Schedule 12 to the Act.
[187] Paragraph 7(k) of Schedule 12 to the Act.
[188] Paragraph 8(2)-(3) of Schedule 12 to the Act.
[189] Paragraph 8(4) of Schedule 12 to the Act.
[190] Paragraph 4(1)(a) of Schedule 12 to the Act.
[191] Paragraph 4(1)(b) of Schedule 12 to the Act.
[192] Paragraph 4(8) of Schedule 12 to the Act.

Typical process

Receiving a notice of audit

7.42 Where we decide to carry out an audit, we will serve the provider of a regulated service with an audit notice.[193] Paragraphs 3.62 - 3.66 above set out guidance regarding how we will serve notices. We will give at least 28 calendar days' notice before we intend to carry out an audit.[194] The audit notice will:

a) specify when the provider must comply with each of the notice's requirements;[195] and
b) explain the consequences of not complying with these requirements.[196]

7.43 After issuing an audit notice, we can revoke it, or change it to make it less onerous.[197]

On the day of the audit

7.44 The specific actions we take during an audit will depend on the individual circumstances of a case. However, the actions we can require a provider to take are:[198]

a) allow us to enter and inspect premises (not domestic premises);
b) allow us to observe the carrying on of its service at the premises;
c) direct us to documents of a specified description on the premises;
d) assist us to view information of a specified description that is capable of being viewed using equipment or a device on the premises;
e) assist us to view, using equipment or a device on the premises, information showing in real time how systems, processes or features of a specified description work;
f) assist us to view, using equipment or a device on the premises, information generated in real time by the performance of a specified test or demonstration;[199]
g) comply with our request for a copy (in whatever form we request) of the documents or information which we have been directed to or which we have been assisted to view;
h) allow us to inspect the documents, information or equipment which we have been directed to or which we have been assisted to view;
i) provide us with an explanation of such documents or information; and
j) allow us to interview a specified number of people of a specified description who are involved in the provision of the service (which does not exceed the number of people who are willing to be interviewed).

[193] Ofcom must serve this notice in accordance with section 208 of the Act.
[194] Paragraph 4(3)(a) of Schedule 12 to the Act.
[195] Paragraph 4(3)(b) of Schedule 12 to the Act.
[196] Paragraph 4(6) of Schedule 12 to the Act.
[197] Paragraph 4(7) of Schedule 12 to the Act.
[198] Paragraph 4(2)(a)-(j) of Schedule 12 to the Act.
[199] Where we require the provider to perform a test or demonstration during an inspection, paragraphs 4.41-4.50 above will apply.

8. Consequences of failure to comply with information gathering powers

Introduction

8.1 It is important that Ofcom's regulatory decisions are founded on a robust evidence base so that we exercise our functions under the Act in a way that is effective and proportionate. Obtaining access to information is fundamental to ensuring Ofcom has a proper appreciation of the factual, economic and legal context within which we exercise our regulatory functions. We will take any failure to comply with our information gathering powers seriously.

8.2 The consequences of a failure to comply could include:

a) enforcement action by Ofcom; or
b) for some of these information gathering powers, criminal liability for business entities and/or individuals.

Enforcement action by Ofcom

8.3 Failing to comply with the information gathering powers granted to Ofcom under the Act may carry significant consequences and may result in Ofcom taking enforcement action.

8.4 We may take enforcement action against providers of regulated services which fail to comply with duties imposed on them in the exercise of our information gathering powers. We may also take enforcement action against:

a) any other person who fails to act in accordance with the requirements of an information notice or to ensure that the information provided is accurate in all material respects; or
b) a person who is required by a skilled person to give assistance to the skilled person but fails to do so.[200]

8.5 When taking enforcement action for non-compliance of such requirements, we will enforce in line with the Act and our Online Safety Enforcement Guidance, which sets out how we decide whether to take enforcement action, and the processes that we would typically follow.[201]

8.6 Enforcement action could result in a decision imposing:

[200] Section 130(3) of the Act.
[201] Online Safety Enforcement Guidance 2024.

a) a financial penalty, which could be a single penalty, a daily penalty, or a combination of the two. We may impose financial penalties up to a maximum of either 10 percent of qualifying worldwide revenue or £18 million (whichever is the greater);[202] and/or
b) requirements to take specified steps to come into compliance and/or remedy the non-compliance.[203]

8.7 Where Ofcom has taken enforcement action against a provider of a regulated service, these measures could be applied to that provider and, if appropriate, also to any other entity related to the provider of the service[204] or an individual controlling the provider of the service.[205] Our Online Safety Enforcement Guidelines provide further information about the circumstances in which a 'Related Company' or 'Controlling Individuals' may be held liable for a failure to comply by a provider of a service.

8.8 Rather than taking separate enforcement action, Ofcom may alternatively take a failure to comply with requirements imposed under our information gathering powers into account when assessing whether a provider of a regulated service has cooperated with an investigation, which is itself an enforceable requirement.[206] Cooperation is a factor we may consider when assessing the appropriate level of any penalty we may decide to impose for a contravention of the regulatory requirement.[207]

8.9 Table 8.1 summarises the information powers that may be subject to enforcement action by Ofcom under the Act.

Table 8.1 Enforceable information powers

Power	Enforceable reqcuirements
Information notices **Section 100 and section 101**	Failure to act in accordance with the requirements of the notice (including responding to an information notice, naming a senior manager, taking steps to enable remote viewing, taking steps to ensure the retention of information, as relevant)[208] Failure to ensure information provided is accurate in all material respects[209]
Skilled persons report **Section 104**	Failure to appoint a skilled person[210] Failure to give the skilled person such assistance as they may reasonably require[211]

[202] Schedule 13 to the Act.
[203] Section 133 of the Act.
[204] That is, a parent company of the service provider, a subsidiary company of the service provider, or a company in the same group as the service provider which has the same parent company as the service provider: see paragraph 1 of Schedule 15 to the Act and the definitions in paragraph 7 of Schedule 15 to the Act.
[205] As defined in the Act: see paragraph 5(4) of Schedule 15 to the Act.
[206] Sections 105(1) and 131 of the Act.
[207] Ofcom, Penalty Guidelines as amended, and the factors listed in paragraph 1.12.
[208] Section 131(2), referring to section 102(8)(a) of the Act.
[209] Section 131(2), referring to section 102(8)(b) of the Act.
[210] Section 131(3)(a), referring to section 104(5)(a) of the Act.
[211] Section 131(2), referring to section 104(7) of the Act.

Power	Enforceable reqcuirements
Entry and inspection **Schedule 12**	Requirements imposed by a person exercising powers to enter and inspect without a warrant[212] Requirements imposed by a person executing a warrant[213]

[212] Section 131(3)(d)(i), referring to paragraph 2 of Schedule 12 to the Act.
[213] Section 131(3)(d)(ii), referring to paragraph 5 of Schedule 12 to the Act.

Criminal liability

8.10 A failure to comply with the requirements of Ofcom's statutory information gathering powers is a criminal offence, subject to the defences set out in the Act. Table 8.2 below provides an overview of these offences and defences and the possible consequences of committing an offence.

8.11 Ofcom has statutory power to bring criminal prosecutions in England and Wales and Northern Ireland for offences relating to matters in relation to which we have functions.[214] We may consider exercising these powers in connection with offences relating to matters covered by this Guidance. We will decide whether to prosecute after considering the guidance set out by the Director of Public Prosecutions in the Code for Crown Prosecutors (England and Wales) or the guidance set out in Section 4 of the Public Prosecution Service Code for Prosecutors (Northern Ireland). For a prosecution to go ahead, we need to be satisfied there is sufficient evidence to provide a realistic prospect of conviction and that a prosecution would be in the public interest.

8.12 In Scotland, we decide whether to report a case to the Procurator Fiscal with a view to prosecution. While Ofcom's views will typically be taken into account, the Procurator Fiscal will decide whether to bring a prosecution based on whether they are satisfied that there is sufficient evidence and that prosecution is in the public interest in accordance with the principles in the Crown Office and Procurator Fiscal Service Prosecution Code.

Table 8.2 Information offences

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
Information notices (Section 100 and section 101)	**Service provider**	**Failure to comply with a requirement of an information notice**	Where Ofcom issues an information notice to the provider of a regulated service and the information notice relates to that provider's service,[215] that provider commits an offence where	• Fine[218] • Court order requiring compliance with the information notice[219]

[214] Section 1(5)(c) of the Communications Act.
[215] See section 109(7) of the Act.
[218] Section 113(1) of the Act.
[219] Section 109(8) of the Act.

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
			they fail to comply with a requirement of an information notice.[216] **Defence:** It is a defence to show that it was not reasonably practicable to comply with the requirements of the information notice at the time required by the notice, but the person has subsequently taken all steps that it was reasonable, and reasonably practicable, to take to comply with those requirements.[217]	
		Knowingly or recklessly providing false information	Where Ofcom issues an information notice to the provider of a regulated service and the information notice relates to that provider's service,[220] that provider commits an offence where they knowingly or recklessly provide information that is false in a material respect. [221]	• Fine[222] • Imprisonment[223] • Court order requiring compliance with the information notice[224]
		Providing an encrypted document or information with	Where Ofcom issues an information notice to the provider of a regulated service and the information notice relates to that provider's service,[225] that provider commits an offence where they provide an encrypted document or information with the	

[216] Section 109(1) of the Act. Pursuant to section 199(1) of the Act, there are certain limits on Ofcom's ability to bring proceedings against a person for an offence under section 109(1), including that Ofcom have given the person a confirmation decision in respect of their failure to comply with the requirements of an information notice which imposes requirements, the time allowed for compliance with the decision has expired without those requirements having been complied with, and Ofcom have not imposed a penalty in respect of the failure to comply with the requirements of an information notice.
[217] Section 109(2) of the Act. If a person relies on this defence, and evidence is adduced which is sufficient to raise an issue with respect to the defence, the court must assume that the defence is satisfied unless the prosecution proves beyond reasonable doubt that it is not: section 201 of the Act.
[220] See section 109(7) of the Act.
[221] Section 109(3) of the Act. However, where a penalty has been imposed on a person in respect of an act or omission constituting an offence under section 109(3), no proceedings may be brought against the person for that offence: section 199(3) of the Act.
[222] Section 113(2) of the Act.
[223] Section 113(2) of the Act.
[224] Section 109(8) of the Act.
[225] See section 109(7) of the Act.

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
		intent to prevent Ofcom from understanding such information	intention of preventing Ofcom from understanding the information.[226]	
		Intentionally preventing information being provided	Where Ofcom issues an information notice to the provider of a regulated service and the information notice relates to that provider's service,[227] that provider commits an offence where they intentionally prevent the information from being provided by suppressing,[228] destroying or altering the information or document (or causing or permitting this to happen).[229]	
		Intentionally deleting or altering information that must be retained pursuant to a Data Retention Notice	Where Ofcom issues a Data Preservation Notice to the provider of a regulated service, that provider commits an offence where they delete[230] or alter information required to be retained by the Data Preservation Notice, and their intention was to prevent the information being available or prevent it being available in unaltered form, for the purpose of an investigation into the child's death.[231]	

[226] Section 109(4) of the Act. However, where a penalty has been imposed on a person in respect of an act or omission constituting an offence under section 109(4), no proceedings may be brought against the person for that offence: section 199(3) of the Act.
[227] See section 109(7) of the Act.
[228] Supressing information or a document includes destroying the means of reproducing information recorded otherwise than in a legible form: section 109(6) of the Act.
[229] Section 109(5) of the Act. However, where a penalty has been imposed on a person in respect of an act or omission constituting an offence under section 109(5), no proceedings may be brought against the person for that offence: section 199(3) of the Act.
[230] Information has been deleted if it is irrecoverable (however that occurred): section 109(6B) of the Act.
[231] Section 109(6A) of the Act.

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
	A person [232]	**Intentionally obstructing or delaying a person from taking copies of documents or requiring an explanation**	Where Ofcom issues an information notice, a person commits an offence if the person intentionally obstructs or delays a person who is taking copies of or extracts from a document produced in response, or requiring an explanation of the document.[233]	• Fine[234] • Imprisonment[235] • Court order requiring the person to permit the making of a copy of a document.[236]
Naming a senior manager (Section 103)	**Named senior manager**	**Failure to take all reasonable steps to prevent entity from committing an offence by failing comply with an information notice**	Where a senior manager has been named pursuant to an information notice, that senior manager commits an offence if the entity has committed an offence by failing to comply with an information notice and the senior manager has failed to take all reasonable steps to prevent that offence being committed.[237] **Defence:** It is a defence to show that the individual was a senior manager within the meaning of section 103 for such a short time after the information notice in question was given	• Fine[240]

[232] As set out in Section 236 of the Act, a "person" includes (in addition to an individual and a body of persons corporate or unincorporate) any organisation or association of persons.
[233] Section 112(1) of the Act.
[234] Section 113(2) of the Act.
[235] Section 113(2) of the Act.
[236] Section 112(4) of the Act.
[237] Section 110(2) of the Act. Pursuant to section 199(2) of the Act, there are certain limits on Ofcom's ability to bring proceedings against a person for an offence under 110(2), including that Ofcom have given the entity a confirmation decision imposing compliance requirements, those requirements have not been complied with, and Ofcom have not imposed a penalty in respect of the failure to comply with the information notice. Further, where a penalty has been imposed on an entity in respect of an act or omission constituting an offence under s 109, no proceedings for an offence under section 110 may be brought against an individual in respect of a failure to prevent that offence: section 199(4) of the Act.
[240] Section 113(1).

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
			that the individual could not reasonably have been expected to take steps to prevent that offence being committed.[238] **Defence:** It is a defence to show that the individual had no knowledge of being named as a senior manager in a response to the information notice in question.[239]	

		Failure to take all reasonable steps to prevent entity from committing other information offences	Where a senior manager has been named pursuant to an information notice, that senior manager commits an offence if the entity commits an offence under:[241]
			a. section 109(3) (false information);
			b. section 109(4) (encrypted information);
			c. section 109(5) (destruction etc of information); or
			d. section 109(6A) (deletion, alteration etc of information);
			and the senior manager failed to take all reasonable steps to prevent that offence from being committed.
			
			Defence: It is a defence to show that the individual was not a senior manager within the meaning of section 103 at the time at which the act constituting the offence occurred.[242]
				• Fine[244]
				• Imprisonment[245]

[238] Section 110(3) of the Act. If a person relies on this defence, and evidence is adduced which is sufficient to raise an issue with respect to the defence, the court must assume that the defence is satisfied unless the prosecution proves beyond reasonable doubt that it is not: section 201 of the Act.
[239] Section 110(8) of the Act. If a person relies on this defence, and evidence is adduced which is sufficient to raise an issue with respect to the defence, the court must assume that the defence is satisfied unless the prosecution proves beyond reasonable doubt that it is not: section 201 of the Act.
[241] Sections 110(4)-(6A).
[242] Section 110(7). If a person relies on this defence, and evidence is adduced which is sufficient to raise an issue with respect to the defence, the court must assume that the defence is satisfied unless the prosecution proves beyond reasonable doubt that it is not: section 201 of the Act.
[244] Section 113(2) of the Act.
[245] Section 113(2) of the Act.

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
			Defence: It is a defence to show that the individual had no knowledge of being named as a senior manager in a response to the information notice in question.[243]	
Interviews **(Section 106)**	**An individual named in an interview notice**	**Failure to attend an interview and answer questions**	If a person[246] fails without reasonable excuse to comply with a requirement to attend an interview and answer questions, they will have committed a criminal offence.[247]	• Fine[248] • Court order requiring the person to comply with a requirement under section 106.[249]
		Knowingly or recklessly providing false information	A person commits an offence if they knowingly or recklessly provide information during an interview that is false in a material respect.[250]	
Audit, entry and inspection (Schedule 12)	**Service provider**	**Failure to comply with a requirement of an audit notice**	A person commits an offence if they fail without reasonable excuse to comply with a requirement of an audit notice.[251]	• Fine[252] • Court order requiring compliance with a requirement of an audit notice.[253]

[243] Section 110(8) of the Act. If a person relies on this defence, and evidence is adduced which is sufficient to raise an issue with respect to the defence, the court must assume that the defence is satisfied unless the prosecution proves beyond reasonable doubt that it is not: section 201 of the Act.

[246] As set out in Section 236 of the Act, a "person" includes (in addition to an individual and a body of persons corporate or unincorporate) any organisation or association of persons.

[247] Section 112(2) of the Act.

[248] Section 113(3) of the Act.

[249] Section 112(4) of the Act.

[250] Section 112(3) of the Act.

[251] Section 111(1) of the Act.

[252] Section 113(1) of the Act.

[253] Section 111(6) of the Act.

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
		Knowingly or recklessly providing false information	A person commits an offence if, in response to an audit notice, they knowingly or recklessly provide information that is false in a material respect.[254]	• Fine[255] • Imprisonment[256] • Court order requiring the person to comply with a requirement of the audit notice or Entry and Inspection Notice.[257]
		Suppressing, destroying or altering information or documents	A person commits an offence if, following an Entry and Inspection Notice, or an audit notice, they: a. suppress, destroy or alter, or cause or permit the suppression, destruction or alteration of, information or documents that Ofcom has required; and b. their intention was to prevent Ofcom from being provided with the information or document in its original form.[258]	
	A person (including individual on the premises or occupier of the premises)	**Intentionally instructing a person acting under Schedule 12**	A person commits an offence if they[193] intentionally obstruct a person acting under Schedule 12 (audit, entry and inspection). [259]	• Imprisonment[260] • Fine[261]

[254] Section 111(2) of the Act.
[255] Section 113(2) of the Act.
[256] Section 113(2) of the Act.
[257] Section 111(6) of the Act.
[258] Section 111(3) of the Act.
[259] Paragraph 18(1)(a) of Schedule 12 to the Act. However, where a penalty has been imposed on a person in respect of an act or omission constituting an offence under paragraph 18 of Schedule 12, no proceedings may be brought against the person for that offence: section 199(3) of the Act.
[260] Paragraph 18(2) of Schedule 12 to the Act.
[261] Paragraph 18(2) of Schedule 12 to the Act.

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
		Failure to comply with a requirement imposed by a person acting under Schedule 12	A person commits an offence if they fail, without reasonable excuse, to comply with any requirement imposed by a person acting under Schedule 12.[262]	
		Providing false information to a person acting under Schedule 12	A person commits an offence if they in response to a requirement imposed by a person acting under Schedule 12, provide information that is false in a material respect, knowing that it is false in a material respect or being reckless as to whether it is false in a material respect. [263]	
Various	**Corporate officers of corporate providers of regulated services**	**Liability of corporate officers for offences committed by corporate providers of regulated services**	Where the provider of a regulated service is a legal person[264] and commits an offence, and it is proved that the offence: a. was committed with the consent or connivance of an officer of the provider, or b. is attributable to any neglect on the part of an officer of the entity; the officer (as well as the entity) commits the offence and is liable to be proceeded against and punished accordingly.[265]	Various (depending on the offence committed).

[262] Paragraph 18(1)(b) of Schedule 12 to the Act. Pursuant to section 199(1) of the Act, there are certain limits on Ofcom's ability to bring proceedings against a person for an offence for failing, without reasonable excuse, to comply with any requirement imposed by a person acting under Schedule 12, including that Ofcom have given the person a confirmation decision in respect of their failure to comply with requirements imposed by a person acting under Schedule 12, that confirmation imposed requirements which have not been complied with, and Ofcom have not imposed a penalty in respect of the failure to comply with the requirements imposed by a person acting under Schedule 12.
[263] Paragraph 18(1)(c) of Schedule 12 to the Act. However, where a penalty has been imposed on a person in respect of an act or omission constituting an offence under paragraph 18 of Schedule 12, no proceedings may be brought against the person for that offence: section 199(3).
[264] Under the law under which it is formed: see section 202(1)(b) of the Act.
[265] Section 202(1)-(2) of the Act. For the definition of 'officer', see sub-sections (3)-(4). Liability is subject to section 199(1) of the Act, which sets out certain conditions that must be fulfilled before proceedings can be brought against a person for an offence under s 109(1) (in relation to information notices) or Schedule 12 paragraph 18(1)(b) (in relation to requirements imposed by a person acting under Schedule 12 e.g. in the course of entering and inspecting premises without a warrant).

Version history

Date	Summary of change	Relevant Ofcom document(s)
[TBC]	Changes to Sections 2, 4 and 8 to reflect amendments to the Online Safety Act 2023 in relation to Data Preservation Notices	[TBC]