

# Draft Online Safety Information Powers Guidance

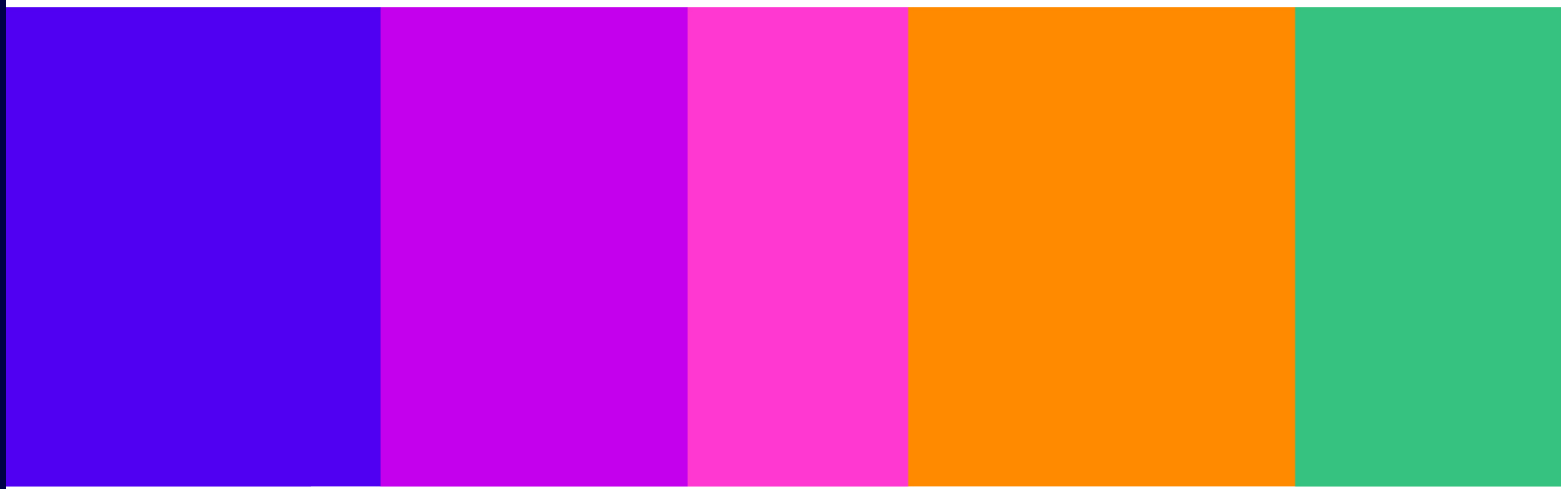
---

Annex 1: Proposed guidance for information gathering powers under the Online Safety Act 2023

## Consultation

Published 26 July 2024

Closing date for responses: 4 October 2024



# Contents

---

## Section

A1. Overview.....	4
A2. Introduction.....	5
The scope of this guidance .....	6
The status of this guidance .....	6
Persons in scope of our information gathering powers .....	7
A3. Ofcom’s general approach to online safety information gathering .....	9
Why Ofcom uses statutory information gathering powers.....	9
Ofcom’s general duties when exercising information gathering powers .....	10
How we will use these powers .....	11
Confidential information .....	12
Disclosure of information .....	13
Record retention and personal data.....	15
Information security .....	17
Service of notices .....	17
A4. Information notices .....	19
Introduction .....	19
When Ofcom may issue information notices under s100, and to whom .....	20
Ofcom’s Information Registry.....	21
Typical process.....	21
Specific considerations for section 100 notices requiring the performance of a test .....	24
Specific considerations for Remote Viewing Information Notices under section 100(3) .....	26
Specific considerations for Coroner Information Notices under section 101(1) .....	30
Naming a senior manager.....	32
A5. Reports by a skilled person under section 104 .....	34
Introduction .....	34
When Ofcom might require a skilled person’s report.....	34

Typical process.....	35
A6. Interviews under section 106.....	37
Introduction .....	37
When Ofcom might require attendance at an interview .....	37
Typical process.....	38
A7. Powers of audit, entry and inspection under Schedule 12.....	40
Introduction .....	40
Home Office code of practice on powers of entry .....	41
Entry and inspection without a warrant.....	41
Entry and inspection with a warrant .....	43
Audit.....	46
A8. Consequences of failure to comply with information gathering powers .....	48
Introduction .....	48
Enforcement action by Ofcom.....	48
Criminal liability .....	51

# 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 draft guidance	Section/ Schedule in the Act	What the section covers (relevant powers)	Location in the draft guidance (paragraph)
<b>Section 2</b>	N/A	Introduction, covering the scope and status of this guidance	A2.1 – A2.12
<b>Section 3</b>	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	A3.1 – A3.54
<b>Section 4</b>	s100 - s103	The power to issue information notices, including:	A4.1 – A4.82
		<ul style="list-style-type: none"> <li>specific considerations for section 100 notices requiring the performance of a test</li> </ul>	A4.34 – A4.44
		<ul style="list-style-type: none"> <li>specific considerations for section 100 notices requiring the remote viewing of certain information under section 100(3) (‘Remote Viewing Information Notice’)</li> </ul>	A4.45 – A4.62
		<ul style="list-style-type: none"> <li>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’<sup>1</sup>)</li> </ul>	A4.63 – A4.76
		<ul style="list-style-type: none"> <li>requirement to name a senior manager under section 103</li> </ul>	A4.77 – A4.82
<b>Section 5</b>	s104	Skilled persons’ reports	A5.1 – A5.17
<b>Section 6</b>	s106	Interviews	A6.1 – A6.18
<b>Section 7</b>	Sch12	Entry, inspection and audit	A7.1 – A7.44
<b>Section 8</b>	N/A	The duties imposed on services and other persons and the consequences of non-compliance with any of these information gathering powers	A8.1 – A8.12

<sup>1</sup> Ofcom may issue an information notice under section 101 for the purpose of responding to a request from information 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.

## The scope of this guidance

---

- 2.4 This guidance covers Ofcom’s information gathering powers as set out in Part 7 Chapter 4 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.<sup>2</sup>
- 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,<sup>3</sup> 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.<sup>4</sup>

## 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 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.
- 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.

---

<sup>2</sup> We are also consulting on a revised version of our [general information gathering policy](#). When we finalise our online safety information gathering guidance, we will include a link to our final general information gathering policy. We also have information on our website: <https://www.ofcom.org.uk/about-ofcom/policies-and-guidelines/information-registry/>

<sup>3</sup> This may include, but is not limited to, other members of the Digital Regulation Cooperation Forum (CMA, FCA and ICO).

<sup>4</sup> Paragraph A3.5 of our [draft online safety enforcement guidance](#) provides examples of sources of information from which Ofcom may receive information used to identify and assess potential compliance issues.

## Persons in scope of our information gathering powers

---

- 2.11 The persons from whom we may gather information differs 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**

<b>Power</b>	<b>(i) Provider of regulated service</b>	<b>(ii) Provider of ancillary service or access facility</b>	<b>(iii) A person who was within (i) or (ii) at a time to which the information relates</b>	<b>(iv) Any other person</b>	<b>(v) Certain individuals connected to regulated services</b>
Section 100 - information notice	X	X	X	X	
Section 100(3) – Remote Viewing Information Notice	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 reasonable and 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:
    - iv) circumstances in which we may disclose information that we have gathered;
    - v) the process we expect to follow if we propose to disclose information; and
    - vi) 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. Our experience is that 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 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 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 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.

- 3.6 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,<sup>5</sup> could be maintained in legal proceedings (in the remainder of this document we refer to this as legally privileged information for convenience).

## Ofcom's general duties when exercising information gathering powers

---

- 3.7 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.
- 3.8 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)).
- 3.9 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.
- 3.10 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.

---

<sup>5</sup> 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.

## How we will use these powers

---

### We will exercise our powers in a reasonable and proportionate way

- 3.11 We will consider on a case-by-case basis whether exercising an information gathering power would be reasonable and proportionate, in line with our regulatory principles to seek the least intrusive regulatory methods of achieving our objectives.<sup>6</sup> 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.
- 3.12 The decision to exercise an information gathering power will be taken by a person with appropriate delegated authority from Ofcom's Board.
- 3.13 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 on the stakeholder involved in collating the information including for example, 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; and
  - f) any other potential costs or other impacts involved 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.
- 3.14 However, in relation to certain decisions, where we intend to rely on information provided by a stakeholder, we will generally obtain it using statutory powers, including:
- a) information provided by a stakeholder that we intend to rely on in published documents such as consultations and statements; and
  - b) information that we intend to rely on in the context of an investigation or a decision that imposes requirements on a stakeholder.
- 3.15 When exercising our information gathering powers we will, to the extent possible, take account of any legislative provisions 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 their ability to respond.

---

<sup>6</sup> 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).

## Information provided voluntarily

- 3.16 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.
  - 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.
- 3.17 If we intend to rely on information provided by a stakeholder on a voluntary basis, we may 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).

## Using information for a different purpose

- 3.18 Where we exercise our information gathering powers, we will explain why we need the required information.<sup>7</sup> Where we have obtained information for a specified purpose and wish to use that information for a different purpose, we will generally either:
- a) explain why we need to use the information for a different purpose and ask for the consent of the provider of the information to use it for this new purpose; and/or
  - b) send the recipient another statutory information notice requiring the same information to be provided for the new purpose. We may also do this where we have informally asked for the provider's consent to use the information for a different purpose, and they have not given consent.

## Confidential information

---

- 3.19 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 which would or might seriously and prejudicially affect the interests of that body or individual.<sup>8</sup>
- 3.20 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. Recipients should clearly identify any such confidential information and explain in writing

---

<sup>7</sup> 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.

<sup>8</sup> Section 149 of the Act.

their reasons for considering it confidential. This includes, 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.

- 3.21 Ofcom will take into consideration any representations made by recipients as to information they consider to be confidential. However, it is for Ofcom to decide what is, and is not, confidential within the statutory definitions, and blanket claims of confidentiality covering entire documents or types of information are unhelpful and unlikely to be accepted. Recipients should therefore identify specific words, numbers, phrases or pieces of information they consider to be confidential.

## Disclosure of information

---

### Circumstances in which we may disclose information that we have gathered

- 3.22 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.
- 3.23 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 our online safety functions. It is a criminal offence for a person to disclose information in contravention of section 393.
- 3.24 The general restriction under section 393 of the Communications Act does not apply in certain circumstances, namely:
- 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.<sup>9</sup>
  - b) when Ofcom is publishing details of enforcement action under the Act. In this circumstance, Ofcom may not publish confidential information.<sup>10</sup>
- 3.25 The Act also enables Ofcom to disclose information to an overseas regulator listed in regulations made by the Secretary of State, to facilitate online safety functions of the overseas regulator which correspond to Ofcom's functions under the Act.<sup>11</sup>

---

<sup>9</sup> 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.

<sup>10</sup> See section 393(6)(a) of the Communications Act and section 149 of the Act.

<sup>11</sup> Section 114 of the Act; see also [The Online Safety \(List of Overseas Regulators\) Regulations 2024](#).

- 3.26 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, where permitted by law, we may disclose such information. For example, it is sometimes permitted and necessary for Ofcom to disclose information to facilitate the carrying out of our functions by ensuring stakeholders can properly understand the basis for our reasoning.<sup>12</sup> We set out from paragraph A3.28 below the process we expect to follow if we propose to disclose information, including information identified as confidential.
- 3.27 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.

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

- 3.28 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.
- 3.29 If Ofcom proposes to disclose information, we will normally first explain our intention to disclose the information and give that person the opportunity to make representations about the proposed disclosure.
- 3.30 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.<sup>13</sup>
- 3.31 Where in order to exercise our functions under the Act there is a need regularly to disclose information, 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.
- 3.32 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 numbers for the purposes of including this in the relevant disclosure, rather than simply removing the information.
- 3.33 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.
- 3.34 Our [draft enforcement guidance](#) provide further information about our approach to disclosing confidential information during an investigation. These would apply to

---

<sup>12</sup> Our regulatory activities should also be transparent and accountable (section 3(3)(a), Communications Act).

<sup>13</sup> Section A10 of our [draft enforcement guidance](#) explains when a procedural complaint can be referred to Ofcom's Procedural Officer and the process for doing so.

information we have obtained for the purposes of an investigation using our information gathering powers.

## Freedom of information requests

- 3.35 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.<sup>14</sup> The applicability of any exemption will depend on the nature of the information sought by any FOI request made.
- 3.36 In particular, section 44 of the FOI Act exempts information from disclosure if its disclosure is prohibited under another enactment.<sup>15</sup> This means that where we have gathered information relating to a particular business using our information gathering powers under the Act, we are prohibited from disclosing that information in response to a FOI request, unless we have that business' consent.
- 3.37 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.
- 3.38 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

---

- 3.39 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](#).
- 3.40 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. Personal data is defined in Article 4 of the UK GDPR as information relating to an identified or identifiable person.<sup>16</sup>
- 3.41 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

---

<sup>14</sup> The Information Commissioner's Office provides guidance on the [exemptions](#) that may apply.

<sup>15</sup> For example, where disclosure is prohibited under section 393 of the Communications Act.

<sup>16</sup> An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person: see [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation).



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.

- 3.42 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.<sup>17</sup>
- 3.43 Those subject to our information gathering powers will be responsible for complying with their own obligations under relevant data protection legislation. 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,<sup>18</sup> including the UK GDPR. However, 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.<sup>19</sup>
- 3.44 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.<sup>20</sup> 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 subject with the required information would seriously impair our ability to achieve the objectives of the processing, or would involve a disproportionate effort,<sup>21</sup> taking account of any measures to protect the data subject's rights, freedoms and legitimate interests.<sup>22</sup> In making that assessment we would take into account that we would not expect to disclose any personal data unless we are satisfied that it is necessary to do so and that we have a legal basis to do so under data protection law.
- 3.45 Ofcom's [General Privacy Statement](#) contains further information about how Ofcom will handle personal data.
- 3.46 At paragraph A4.56 below we set out some further guidance regarding personal data in the context of Remote Viewing Information Notices under section 100(3).

---

<sup>17</sup> 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'.

<sup>18</sup> UK data protection legislation means the legislation identified in section 3(9) of the Data Protection Act 2018.

<sup>19</sup> 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).

<sup>20</sup> UK GDPR, Article 14(1)-(3).

<sup>21</sup> UK GDPR, Article 14(5).

<sup>22</sup> 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](#).



## Information security

---

- 3.47 Ensuring information is appropriately protected is central to Ofcom’s work and our reputation as the UK’s communications regulator.
- 3.48 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](#).
- 3.49 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

---

- 3.50 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.<sup>23</sup> Where that is the case, we may give a notice to that person by:<sup>24</sup>
- a) delivering it by hand;
  - b) leaving it, or sending it by post<sup>25</sup> to, that person’s ‘proper address’; or
  - c) sending it by email to the person’s email address.<sup>26</sup>
- 3.51 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<sup>27</sup> or other officer<sup>28</sup> of that entity.<sup>29</sup>

---

<sup>23</sup> 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.

<sup>24</sup> Section 208(1)-(2) of the Act.

<sup>25</sup> 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.

<sup>26</sup> 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.

<sup>27</sup> A director includes any person occupying the position of a director, by whatever name called: see section 208(12) of the Act.

<sup>28</sup> 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.

<sup>29</sup> Section 208(6) of the Act.

- 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.<sup>30</sup> 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;<sup>31</sup>
  - ii) where the person is not an entity, the person's last known address.<sup>32</sup> In the case of a notice to an individual requiring them to attend an interview,<sup>33</sup> 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.<sup>34</sup>

3.52 The Act also specifies what the person's email address is in different scenarios, namely:<sup>35</sup>

- 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.

3.53 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 information proving the contrary.<sup>36</sup> 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.

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

---

<sup>30</sup> Section 208(7) of the Act.

<sup>31</sup> Section 208(8) of the Act.

<sup>32</sup> Section 208(7) of the Act.

<sup>33</sup> Under section 108 of the Act.

<sup>34</sup> Section 208(9) of the Act.

<sup>35</sup> Section 208(10) of the Act.

<sup>36</sup> 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 A4.10 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(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.
- 4.6 **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.
- 4.7 This part of the guidance covers:
- a) when we may issue information notices under section 100, and to whom;
  - 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 Coroner Information Notices under section 101(1); and
  - g) requirement to name a senior manager.

## When Ofcom may issue information notices under s100, and to whom

---

- 4.8 Section 100 of the Act grants us the power to require information from certain persons by way of a statutory notice.<sup>37</sup>
- 4.9 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.
- 4.10 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<sup>38</sup> in relation to a regulated service;
  - d) a person who provides an access facility<sup>39</sup> 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.<sup>40</sup>
- 4.11 We may only issue an information notice where this is proportionate to the use of the information being gathered.<sup>41</sup> We set out further detail about the principle of proportionality from paragraph A3.11 above.
- 4.12 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, preparing a code of practice, and carrying out research or preparing a report in relation to online safety matters.
- 4.13 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.<sup>42</sup>
- 4.14 An information notice issued under section 100 may require the production of documents wherever those documents are held, including outside the UK.<sup>43</sup>

---

<sup>37</sup> Section 102(1) of the Act

<sup>38</sup> Under section 145(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)

<sup>39</sup> Under section 147(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.

<sup>40</sup> Section 100(5) of the Act

<sup>41</sup> Section 100(4) of the Act.

<sup>42</sup> Sections 100(2)(a) and (b) of the Act.

<sup>43</sup> Section 204(2) of the Act.

## Ofcom's Information Registry

---

- 4.15 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<sup>44</sup> which is overseen by Ofcom's Enforcement Director.
- 4.16 The Information Registry was set up in May 2020 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.
- 4.17 The Information Registry supports project teams across Ofcom by preparing, issuing and tracking information requests and gathering responses.
- 4.18 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 allows for consideration to be given to other regulatory activity and will ensure Ofcom sets a reasonable deadline to respond.
- 4.19 The Information Registry maintains up-to-date external stakeholder information, including contact details and corporate structure information.
- 4.20 The Information Registry will engage regularly with stakeholders to raise any issues and can offer support and introductory meetings to new or smaller stakeholders where required.
- 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.

## Typical process

---

### Draft information notices

- 4.22 Ofcom will, as a general rule, issue 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.
- 4.23 Where Ofcom issues an 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.

---

<sup>44</sup> The Information Registry was launched in 2020. Further information on the Information Registry and our statutory information gathering processes can be found on the [Ofcom website](#).

- 4.24 However, there are times when it is likely to be appropriate to issue an information notice without engaging with the recipient first. 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) 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;
  - c) where information has been provided to Ofcom previously on an informal/voluntary basis;
  - d) where we are asking for updates to information previously provided, where questions are the same as, or very similar to, questions previously asked;
  - e) where we are issuing a similar statutory information notice to a large number of stakeholders, such that preliminary engagement is not practicable; and
  - f) 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

- 4.25 Paragraphs **Error! Reference source not found.**<sup>50</sup> - **Error! Reference source not found.**<sup>54</sup> above set out guidance regarding how we will serve notices, including information notices.

## Contents of the notice

- 4.26 An information notice 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.

## Responding to the notice

### Recipients must provide complete and accurate information

- 4.27 The recipient of an information notice is under a legal duty to act in accordance with the requirements of the notice, and to ensure that the information provided is accurate in all material respects.<sup>45</sup> 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.

Section A8 of this guidance sets out the consequences of non-compliance with our information gathering powers in more detail.

- 4.28 On receipt of an information notice, the recipient should:
- a) review the request and **acknowledge receipt** of it to Ofcom;

---

<sup>45</sup> Section 100(8) of the Act

- 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 Ofcom as soon as possible;
  - c) consider the response and **locate or generate any information required**, 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.
- 4.29 Before the recipient sends its response to Ofcom, they should make sure that:
- 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 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) the response provided is **clear, complete, and accurate**. If the recipient has any doubts about the accuracy of the information in your 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.
- 4.30 The recipient should check the completeness and accuracy of the information provided prior to responding to the notice. For established businesses, a governance check should 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.

### Respond by the required deadline

- 4.31 The recipient must send the response by the deadline given in the 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. We will only agree to extend deadlines where there is good reason for doing so, like 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.
- 4.32 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 would need to be generated), and shorter timeframes for information that may be quicker to collect or produce.

## Withdrawing an information notice

- 4.33 We may withdraw an information notice by giving notice to the recipient.<sup>46</sup> When doing so, Ofcom will confirm that no further action is needed.

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

---

- 4.34 As part of an information notice under section 100(1), Ofcom may require the recipient to generate information.<sup>47</sup> We may require the recipient to do this by performing a test.<sup>48</sup> 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.
- 4.35 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.<sup>49</sup> We set out further detail about the principle of proportionality from paragraph A3.11 above.
- 4.36 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).
- 4.37 From paragraphs A4.45 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

- 4.38 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.

### Test datasets

- 4.39 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

---

<sup>46</sup> Section 102(9) provides that Ofcom may cancel an information notice by notice to the person to whom it was given.

<sup>47</sup> Section 100(2)(a) of the Act.

<sup>48</sup> 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)'.

<sup>49</sup> Section 100(4) of the Act.



the outputs are relevant to the specific function that we are exercising or considering exercising.

- 4.40 We may ask a recipient to conduct a test using a test dataset provided by Ofcom.<sup>50</sup> We are more likely to take this approach in cases where we are conducting benchmark testing in relation to specific user characteristics, such as age (for purposes of testing the effectiveness of a service's age estimation technology). 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.
- 4.41 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

- 4.42 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. We will generally request that a test or demonstration is undertaken on such an environment where it is available. However, if a test environment is unavailable, we may request a test using the 'live' service environment. In this circumstance, any data processing by the recipient of the notice would need to comply with data protection law. As noted above at paragraph A3.43, 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.<sup>51</sup>

### Information generated by the test

- 4.43 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.
- 4.44 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 A3.42, we will seek to limit the personal data which we require to that which is necessary for the performance of our functions under the

---

<sup>50</sup> 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'.

<sup>51</sup> 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).

Act. Further, as noted at paragraph A3.15, 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)

---

- 4.45 The Act places several duties on regulated services regarding the algorithms used to deliver their services. For example, the safety and protection of children duties require user-to-user services to use proportionate measures to mitigate the risk of individuals encountering illegal and harmful content, 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.
- 4.46 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.
- 4.47 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.<sup>52</sup>
- 4.48 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.
- 4.49 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.<sup>53</sup>
- 4.50 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.<sup>54</sup> We set out further detail about the principle of proportionality from paragraph 3.11 above.
- 4.51 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 A7 below).<sup>55</sup> Further, Ofcom’s power to enter and inspect premises without a warrant includes a power to view, using equipment or

---

<sup>52</sup> Section 100(3) of the Act.

<sup>53</sup> Pursuant to s 100(3) of the Act, Ofcom may only exercise this power in relation to a person falling within sections (5)(a)-(d).

<sup>54</sup> Section 100(4) of the Act.

<sup>55</sup> 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.

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.<sup>56</sup>

- 4.52 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 A3 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.<sup>57</sup>
- 4.53 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.

## Demonstrations and tests

- 4.54 Where, as part of a Remote Viewing Information Notice, we require the performance of a test or demonstration, the considerations set out at paragraphs A4.344 - A4.43 in relation to the performance of a test will apply.
- 4.55 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, nor could we require companies providing infrastructure services to create the means to weaken or circumvent cybersecurity measures such as encryption.<sup>58</sup> 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 A4.43 above), we will only be able to view such a test and any data processing would need to comply with data

---

<sup>56</sup> Provided that the recipient is a person referred to in section 100(5)(a)-(d).

<sup>57</sup> 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'.

<sup>58</sup> 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'.

protection law. Lastly, we would expect to communicate regularly with the service's employees during the process of remotely viewing a test or demonstration.

## Data protection considerations

- 4.56 Where we exercise this power, it is possible that the information we seek to remotely view may include personal data. Consistent with paragraph A3.42 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.

## Receiving a Remote Viewing Information Notice

- 4.57 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.<sup>59</sup>
- 4.58 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.
- 4.59 In line with our general process for issuing information notices, we would expect to send a draft of the Remote Viewing Information Notice<sup>60</sup> 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.
- 4.60 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

- 4.61 The recipient of a Remote Viewing Information Notice should take the steps set out in paragraph A4.28 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.

---

<sup>59</sup> Section 102(5) of the Act.

<sup>60</sup> Paragraph A4.24 above sets out some examples of time when it is likely to be appropriate to issue an information notice without engaging with the recipient first.

- 4.62 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 A4.2928 above.

## 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

- 4.63 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.<sup>61</sup>
- 4.64 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.
- 4.65 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.<sup>62</sup>
- 4.66 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.
- 4.67 As with information notices issued under section 100 (see paragraph A4.14.14 above), Coroner Information Notices may require the production of documents held outside the UK.<sup>63</sup>
- 4.68 Our typical process explained at paragraphs A4.22 - A4.33 will also apply when we issue a Coroner Information Notice under section 101(1).

---

<sup>61</sup> Schedule 5, paragraph 1(2) Coroners and Justice Act 2009; Section 17A(2) Coroners Act (Northern Ireland) 1959 (c. 15 (N.I.)).

<sup>62</sup> Section 101(7) of the Act.

<sup>63</sup> Section 204(2) of the Act.

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

- 4.69 Ofcom has discretion to issue a Coroner Information Notice for the purpose of responding to a request from a coroner.
- 4.70 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.<sup>64</sup> 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, including what personal information is needed;
  - 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.
- 4.71 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.
- 4.72 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. 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.
- 4.73 Coroners who wish to discuss a potential request with us should contact [CoronersSupport@ofcom.org.uk](mailto: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

- 4.74 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.

---

<sup>64</sup> [Guidance No 46 Obtaining information regarding social media use - Courts and Tribunals Judiciary](#)

## Disclosure of information obtained under a Coroner Information Notice

- 4.75 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.<sup>65</sup> The notice will inform the recipient that we intend to take this approach.
- 4.76 Further, we will generally specify in the 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. 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.<sup>66</sup> We generally will not review or analyse the information provided, except to ensure it is complete.

## Naming a senior manager

---

- 4.77 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.<sup>67</sup>
- 4.78 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.<sup>68</sup>
- 4.79 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.
- 4.80 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.
- 4.81 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).<sup>69</sup> If the named senior manager fails to take all reasonable steps to prevent that

---

<sup>65</sup> 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 2003, in particular sub-sections (2)(b), (3)(ha)-(hb), (4) and (5)(ca), (nb) and (s).

<sup>66</sup> 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.

<sup>67</sup> Section 103(1)-(2) of the Act.

<sup>68</sup> Section 103(4) and (5) of the Act.

<sup>69</sup> See section 109(1) of the Act; and further section A8 below.



offence being committed, they will also have committed an offence.<sup>70</sup> 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;<sup>71</sup>
- 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;<sup>72</sup> or
- c) intentionally preventing the information from being provided by suppressing, destroying or altering the information or document (or causing or permitting this to happen);<sup>73</sup>

and that senior manager failed to take all reasonable steps to prevent that offence being committed, then that senior manager will have committed an offence.<sup>74</sup> More information about the consequences for non-compliance can be found in section A8, including information about defences that may be available to named senior managers in the event they are prosecuted for a criminal offence.

- 4.82 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.<sup>75</sup> 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.<sup>76</sup> 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.<sup>77</sup>

---

<sup>70</sup> Section 110(2) of the Act. See further section A8 below.

<sup>71</sup> Such that the entity commits an offence under section 109(3) of the Act; see further section A8 below.

<sup>72</sup> Such that the entity commits an offence under section 109(4) of the Act; see further section A8 below.

<sup>73</sup> Such that the entity commits an offence under section 109(5) of the Act; see further section A8 below.

<sup>74</sup> Sections 110(4), (5) and (6) of the Act. See further section A8 below.

<sup>75</sup> Section 103(3)(a) of the Act.

<sup>76</sup> 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).

<sup>77</sup> 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.<sup>78</sup>
- 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'<sup>79</sup>; or
  - b) develop our understanding of the nature and level of risk of such a compliance failure, and ways to mitigate that risk.<sup>80</sup>
- 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.<sup>81</sup>
- 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.<sup>82</sup> 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.

---

<sup>78</sup> Section 104(6) of the Act.

<sup>79</sup> 'Relevant requirement' is defined in section 104(13) of the Act. The relevant requirements include:

- a) duties to carry out risk assessments;
- b) duties in relation to illegal content;
- c) duties in relation to content reporting;
- d) duties in relation to content which is harmful to children;
- e) user empowerment duties for Category 1 services, i.e. including features which adult users may use or apply, if they wish to increase their control over certain content;
- f) duties which apply to Category 1 and 2A services to ensure they have systems and processes in place to prevent users from encountering fraudulent advertisements; and
- g) duties in relation to the reporting of CSEA content to the National Crime Agency.

<sup>80</sup> Section 104(1) of the Act; see also section 104(2).

<sup>81</sup> Sections 104(3) and 122 of the Act.

<sup>82</sup> Section 104(6) of the Act.

- 5.6 The following are examples of when we may consider it necessary to exercise our power to obtain a skilled person's report:
- 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.
- 5.7 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.
- 5.8 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

---

- 5.9 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.
- 5.10 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 A5.14(a) and (b) below for further detail).
- 5.11 Paragraphs A3.50 – A3.54 above set out guidance regarding how we will serve notices, including the notices referred to in the paragraph above.
- 5.12 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.<sup>83</sup>
- 5.13 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 we are

---

<sup>83</sup> Section 104(4) and (5).

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.<sup>84</sup>

- 5.14 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.
- 5.15 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.
- 5.16 The service provider and anyone who works for the service (or 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.<sup>85</sup>
- 5.17 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.<sup>86</sup> If the provider of the service fails to make payment, the amount due can be recovered by order of court.<sup>87</sup>

---

<sup>84</sup> 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).

<sup>85</sup> Section 104(7) of the Act

<sup>86</sup> Section 104(8) of the Act.

<sup>87</sup> Section 104(9)-(12) of the Act.

# 6. Interviews under section 106

## Introduction

---

- 6.1 Where a 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, we may decide to open an investigation.<sup>88</sup> 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.<sup>89</sup>
- 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 individuals whom 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.<sup>90</sup>
- 6.6 We can require such an individual to attend an interview even if they are outside the UK.<sup>91</sup>
- 6.7 If Ofcom requires an individual to attend an interview, that individual is not required to disclose legally privileged information to Ofcom.<sup>92</sup>
- 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.

---

<sup>88</sup> Section 105 of the Act.

<sup>89</sup> Section 106 of the Act.

<sup>90</sup> Section 106(4) of the Act

<sup>91</sup> Section 204(3) of the Act

<sup>92</sup> Section 106(6) of the Act.

## Typical process

---

- 6.9 We will give the individual a notice requiring them to attend at a specified time and place, and to answer questions and provide explanations about any relevant matter.<sup>93</sup> The notice will set out the subject matter and purpose of the interview and contain information about the consequences of non-compliance.<sup>94</sup>
- 6.10 Paragraphs A3.50 - **Error! Reference source not found.**<sup>54</sup> 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.<sup>95</sup>
- 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.<sup>96</sup>
- 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 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 advisor when answering our questions. Reasonable breaks in the interview can be requested to allow time for the person to talk with their legal advisor.

---

<sup>93</sup> Section 106(2) of the Act.

<sup>94</sup> Section 106(3) of the Act.

<sup>95</sup> Section 208(9) of the Act.

<sup>96</sup> Section 106(5) of the Act.

6.18 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;<sup>97</sup>
  - b) apply for and execute a warrant to enter and inspect certain premises;<sup>98</sup> and/or
  - c) carry out audits on a service (which may also involve entering and inspecting premises).<sup>99</sup>
- 7.2 In general, our use of powers of entry, inspection and audit will typically be reserved for more serious or complex cases. 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.
- 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.<sup>100</sup> We cannot exercise these powers, or our audit power, in relation to domestic premises.<sup>101</sup> We also cannot exercise these powers to require the disclosure of information or documents which are legally privileged.<sup>102</sup>
- 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 chapter.<sup>103</sup>
- 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.
- 7.6 Section 8 of this guidance sets out the consequences of non-compliance with our audit, entry and inspection powers in more detail.

---

<sup>97</sup> Paragraphs 2-3 of Schedule 12 to the Act.

<sup>98</sup> 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.

<sup>99</sup> Paragraph 4 of Schedule 12 to the Act.

<sup>100</sup> Paragraphs 2(1)(a) and 5(1)(a) of Schedule 12 to the Act.

<sup>101</sup> 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.

<sup>102</sup> Paragraphs 4(5) and 17(3) of Schedule 12 to the Act.

<sup>103</sup> See paragraph 1 of Schedule 12 to the Act.



## 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.<sup>104</sup> 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.<sup>105</sup> However, we may only exercise these powers so far as is required in connection with those functions, and not further.<sup>106</sup>
- 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.

### 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

---

<sup>104</sup> The [Code](#), paragraph 5.1.

<sup>105</sup> Paragraph 2(7) of Schedule 12 to the Act.

<sup>106</sup> Paragraph 2(7) of Schedule 12 to the Act.

occupier<sup>107</sup> 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').<sup>108</sup>

- 7.14 The Entry and Inspection Notice will include details of the following:
- the date, time and purpose of the proposed entry;<sup>109</sup>
  - that the entry will be conducted without a warrant;
  - the powers we will be exercising;
  - the occupier's rights;
  - any compensation or complaints procedures that exist; and
  - where a copy of the Code may be obtained.<sup>110</sup>
- 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;<sup>111</sup> and
  - d) the consequences of not complying with the requirements outlined in the notice.
- 7.16 Paragraphs **Error! Reference source not found.** - **Error! Reference source not found.**<sup>54</sup> 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.<sup>112</sup> We will determine what constitutes a 'reasonable hour' by reference to the normal working practices of the particular business concerned.<sup>113</sup>
- 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.<sup>114</sup>
- 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 enabling us to exercise our power of entry and inspection without a warrant effectively.<sup>115</sup>
- 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

---

<sup>107</sup> The [Code](#) defines 'occupier' as a person who is or appears to be in charge of the premises: paragraph 4.8.

<sup>108</sup> Paragraph 2(1)(b) of Schedule 12 to the Act.

<sup>109</sup> The [Code](#), paragraph 8.2.

<sup>110</sup> The [Code](#), paragraph 7.3.

<sup>111</sup> Where we require the occupier to perform a test or demonstration during an inspection, paragraphs A4.38-A4.44 above will apply.

<sup>112</sup> Paragraph 2(2) of Schedule 12 to the Act.

<sup>113</sup> The [Code](#), paragraph 13.1.

<sup>114</sup> Paragraph 2(3) of Schedule 12 to the Act.

<sup>115</sup> The [Code](#), paragraph 9.1.

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:<sup>116</sup>
- 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;<sup>117</sup>
  - 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 powers (a)-(f) above.<sup>118</sup>
- 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.<sup>119</sup>
- 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.<sup>120</sup> 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.<sup>121</sup>
- 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);<sup>122</sup>

---

<sup>116</sup> Paragraphs 2(4)(a)-(f) of Schedule 12 to the Act.

<sup>117</sup> As noted above, where we require the occupier to perform a test or demonstration during an inspection, paragraphs A4.38 - A4.44 above will apply.

<sup>118</sup> Paragraph 2(6) of Schedule 12 to the Act.

<sup>119</sup> The [Code](#), paragraph 18.1.

<sup>120</sup> Paragraph 18(1) of Schedule 12 to the Act.

<sup>121</sup> Paragraph 5 of Schedule 12 to the Act.

<sup>122</sup> Paragraph 5(1)(a) and 17(2) of Schedule 12 to the Act.

- b) there are reasonable grounds to suspect that the provider is failing or has failed to comply with an enforceable requirement,<sup>123</sup>
- 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:<sup>124</sup>
  - 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.<sup>125</sup> A warrant authorises us to enter premises on one occasion only, unless it specifies that it authorises multiple entries.<sup>126</sup>

## Typical process

### Before we enter

7.29 We will only exercise this power at a reasonable hour,<sup>127</sup> unless it appears that the purpose of the search would be frustrated or seriously prejudiced by entering at a reasonable hour.<sup>128</sup>

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.<sup>129</sup> During this time, authorised persons may take necessary measures to prevent tampering with evidence.<sup>130</sup>

---

<sup>123</sup> Paragraph 21 of Schedule 12 to the Act sets out the definition of ‘enforceable requirement’ that applies in this context.

<sup>124</sup> Paragraph 5(2) of Schedule 12 to the Act.

<sup>125</sup> Paragraph 10 of Schedule 12 to the Act.

<sup>126</sup> Paragraph 14 of Schedule 12 to the Act.

<sup>127</sup> A reasonable hour will be determined by reference to the normal working practices of the particular business concerned. The [Code](#), paragraph 13.1.

<sup>128</sup> Paragraph 9 of Schedule 12 to the Act.

<sup>129</sup> A “reasonable time” means such period of time as the authorised person considers is reasonable in the circumstances.

<sup>130</sup> 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.

- 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.<sup>131</sup>
- 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.<sup>132</sup>
- 7.33 We may use reasonable force to facilitate us exercising our powers under a warrant if necessary,<sup>133</sup> 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,<sup>134</sup> and leave the premises as effectively secured against trespassers as it was when we arrived.<sup>135</sup>

### 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.<sup>136</sup> 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 A7.37 below, as long as they are in the company and under the supervision of a person authorised under the warrant.<sup>137</sup>

### 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;
  - 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);

---

<sup>131</sup> Paragraph 6(1)(a)-(b) of Schedule 12 to the Act.

<sup>132</sup> Paragraph 6(1)(c) of Schedule 12 to the Act.

<sup>133</sup> Paragraph 13 of Schedule 12 to the Act.

<sup>134</sup> Paragraph 6(2) of Schedule 12 to the Act.

<sup>135</sup> Paragraph 15 of Schedule 12 to the Act.

<sup>136</sup> Paragraph 11 of Schedule 12 to the Act.

<sup>137</sup> Paragraph 12 of Schedule 12 to the Act.

- 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.<sup>138</sup>

### Our powers of seizure

- 7.38 As noted at paragraph A7.37k)) 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.<sup>139</sup>
- 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.<sup>140</sup> We can retain anything we seize under a warrant for as long as we think is necessary.<sup>141</sup>

## 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.<sup>142</sup> 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.<sup>143</sup>
- 7.41 We may require a provider to pay some, or all, of the reasonable costs of an audit.<sup>144</sup>

### 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.<sup>145</sup> Paragraphs **Error! Reference source not found.50 - Error! Reference source not found.54** 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.<sup>146</sup> The audit notice will:

---

<sup>138</sup> Paragraph 7 of Schedule 12 to the Act.

<sup>139</sup> Paragraph 7(k) of Schedule 12 to the Act.

<sup>140</sup> Paragraph 8(2)-(3) of Schedule 12 to the Act.

<sup>141</sup> Paragraph 8(4) of Schedule 12 to the Act.

<sup>142</sup> Paragraph 4(1)(a) of Schedule 12 to the Act.

<sup>143</sup> Paragraph 4(1)(b) of Schedule 12 to the Act.

<sup>144</sup> Paragraph 4(8) of Schedule 12 to the Act.

<sup>145</sup> Ofcom must serve this notice in accordance with section 208 of the Act.

<sup>146</sup> Paragraph 4(3)(a) of Schedule 12 to the Act.

- a) specify when the provider must comply with each of the notice's requirements;<sup>147</sup> and
- b) explain the consequences of not complying with these requirements.<sup>148</sup>

7.43 After issuing an audit notice, we can revoke it, or change it to make it less onerous.<sup>149</sup>

### 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:<sup>150</sup>

- 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;<sup>151</sup>
- 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).

---

<sup>147</sup> Paragraph 4(3)(b) of Schedule 12 to the Act.

<sup>148</sup> Paragraph 4(6) of Schedule 12 to the Act.

<sup>149</sup> Paragraph 4(7) of Schedule 12 to the Act.

<sup>150</sup> Paragraph 4(2)(a)-(j) of Schedule 12 to the Act.

<sup>151</sup> Where we require the provider to perform a test or demonstration during an inspection, paragraphs A4.3838-A4.44 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.<sup>152</sup>
- 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.<sup>153</sup>
- 8.6 Enforcement action could result in a decision imposing:
- 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),<sup>154</sup> and/or

---

<sup>152</sup> Section 130(3) of the Act.

<sup>153</sup> Ofcom, [‘Protecting people from illegal harms online: Annex 11: Enforcement guidance \(draft for consultation\)’](#), (9 November 2023).

<sup>154</sup> Schedule 13 to the Act.



- b) requirements to take specified steps to come into compliance and/or remedy the non-compliance.<sup>155</sup>
- 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<sup>156</sup> or an individual controlling the provider of the service.<sup>157</sup> 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.<sup>158</sup> 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.<sup>159</sup>
- 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 requirements
<b>Information notices</b> <b>Section 100 and section 101</b>	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, etc as relevant) <sup>160</sup>  Failure to ensure information provided is accurate in all material respects <sup>161</sup>
<b>Skilled persons report</b> <b>Section 104</b>	Failure to appoint a skilled person <sup>162</sup> Failure to give the skilled person such assistance as they may reasonably require <sup>163</sup>

<sup>155</sup> Section 133 of the Act.

<sup>156</sup> 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.

<sup>157</sup> As defined in the Act: see paragraph 5(4) of Schedule 15 to the Act.

<sup>158</sup> Sections 105(1) and 131 of the Act.

<sup>159</sup> Ofcom, [Penalty Guidelines](#) as amended, and the factors listed in paragraph 1.12.

<sup>160</sup> Section 131(2), referring to section 102(8)(a) of the Act.

<sup>161</sup> Section 131(2), referring to section 102(8)(b) of the Act.

<sup>162</sup> Section 131(3)(a), referring to section 104(5)(a) of the Act.

<sup>163</sup> Section 131(2), referring to section 104(7) of the Act.

Power	Enforceable requirements
<p data-bbox="245 309 501 340"><b>Entry and inspection</b></p> <p data-bbox="298 365 448 396"><b>Schedule 12</b></p>	<p data-bbox="576 262 1378 331">Requirements imposed by a person exercising powers to enter and inspect without a warrant<sup>164</sup></p> <p data-bbox="628 409 1326 441">Requirements imposed by a person executing a warrant<sup>165</sup></p>

---

<sup>164</sup> Section 131(3)(d)(i), referring to paragraph 2 of Schedule 12 to the Act.

<sup>165</sup> 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 8.1 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.<sup>166</sup> 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
<b>Information notices (Section 100 and section 101)</b>	<b>Service provider</b>	<b>Failure to comply with a requirement of an information notice</b>	Where Ofcom issues an information notice to the provider of a regulated service and the information notice relates to that provider’s service, <sup>167</sup> that provider commits an offence where they fail to comply with a requirement of an information notice. <sup>168</sup>	<ul style="list-style-type: none"> <li>• Fine<sup>170</sup></li> <li>• Court order requiring compliance with the information notice<sup>171</sup></li> </ul>

<sup>166</sup> Section 1(5)(c) of the Communications Act.

<sup>167</sup> See section 109(7) of the Act.

<sup>168</sup> 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.

<sup>170</sup> Section 113(1) of the Act.

<sup>171</sup> Section 109(8) of the Act.

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
			<b>Defence:</b> 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 reasonable steps to comply with those requirements. <sup>169</sup>	
		<b>Knowingly or recklessly providing false information</b>	Where Ofcom issues an information notice to the provider of a regulated service and the information notice relates to that provider's service, <sup>172</sup> that provider commits an offence where they knowingly or recklessly provide information that is false in a material respect. <sup>173</sup>	<ul style="list-style-type: none"> <li>• Fine<sup>174</sup></li> <li>• Imprisonment<sup>175</sup></li> <li>• Court order requiring compliance with the information notice<sup>176</sup></li> </ul>
		<b>Providing an encrypted document or information with intent to prevent Ofcom from understanding such information</b>	Where Ofcom issues an information notice to the provider of a regulated service and the information notice relates to that provider's service, <sup>177</sup> that provider commits an offence where they provide an encrypted document or information with the intention of preventing Ofcom from understanding the information. <sup>178</sup>	

<sup>169</sup> 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.

<sup>172</sup> See section 109(7) of the Act.

<sup>173</sup> 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.

<sup>174</sup> Section 113(2) of the Act.

<sup>175</sup> Section 113(2) of the Act.

<sup>176</sup> Section 109(8) of the Act.

<sup>177</sup> See section 109(7) of the Act.

<sup>178</sup> 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.

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
		<b>Intentionally preventing information being provided</b>	Where Ofcom issues an information notice to the provider of a regulated service and the information notice relates to that provider's service, <sup>179</sup> that provider commits an offence where they intentionally prevent the information from being provided by suppressing, <sup>180</sup> destroying or altering the information or document (or causing or permitting this to happen). <sup>181</sup>	
	<b>A person</b> <sup>182</sup>	<b>Intentionally obstructing or delaying a person from taking copies of documents or requiring an explanation</b>	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. <sup>183</sup>	<ul style="list-style-type: none"> <li>• Fine<sup>184</sup></li> <li>• Imprisonment<sup>185</sup></li> <li>• Court order requiring the person to permit the making of a copy of a document.<sup>186</sup></li> </ul>
<b>Naming a senior manager (Section 103)</b>	<b>Named senior manager</b>	<b>Failure to take all reasonable steps to prevent entity from committing an</b>	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	<ul style="list-style-type: none"> <li>• Fine<sup>190</sup></li> </ul>

<sup>179</sup> See section 109(7) of the Act.

<sup>180</sup> Suppressing information or a document includes destroying the means of reproducing information recorded otherwise than in a legible form: section 109(6) of the Act.

<sup>181</sup> 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.

<sup>182</sup> 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.

<sup>183</sup> Section 112(1) of the Act.

<sup>184</sup> Section 113(2) of the Act.

<sup>185</sup> Section 113(2) of the Act.

<sup>186</sup> Section 112(4) of the Act.

<sup>190</sup> Section 113(1).

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
		<b>offence by failing comply with an information notice</b>	<p>take all reasonable steps to prevent that offence being committed.<sup>187</sup></p> <p><b>Defence:</b> 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 that the individual could not reasonably have been expected to take steps to prevent that offence being committed.<sup>188</sup></p> <p><b>Defence:</b> 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.<sup>189</sup></p>	
		<b>Failure to take all reasonable steps to prevent entity from committing other information offences</b>	<p>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:<sup>191</sup></p> <ol style="list-style-type: none"> <li>a. section 109(3) (false information);</li> <li>b. section 109(4) (encrypted information); or</li> <li>c. section 109(5) (destruction etc of information);</li> </ol>	<ul style="list-style-type: none"> <li>• Fine<sup>194</sup></li> <li>• Imprisonment<sup>195</sup></li> </ul>

<sup>187</sup> 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.

<sup>188</sup> 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.

<sup>189</sup> 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.

<sup>191</sup> Sections 110(4) and (5).

<sup>194</sup> Section 113(2) of the Act.

<sup>195</sup> Section 113(2) of the Act.

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
			<p>and the senior manager failed to take all reasonable steps to prevent that offence from being committed.</p> <p><b>Defence:</b> 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.<sup>192</sup></p> <p><b>Defence:</b> 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.<sup>193</sup></p>	
<b>Interviews (Section 106)</b>	<b>An individual named in an interview notice</b>	<b>Failure to attend an interview and answer questions</b>	If a person <sup>196</sup> fails without reasonable excuse to comply with a requirement to attend an interview and answer questions, they will have committed a criminal offence. <sup>197</sup>	<ul style="list-style-type: none"> <li>• Fine<sup>198</sup></li> <li>• Court order requiring the person to comply with a requirement under section 106.<sup>199</sup></li> </ul>
		<b>Knowingly or recklessly providing false information</b>	A person commits an offence if they knowingly or recklessly provide information during an interview that is false in a material respect. <sup>200</sup>	

<sup>192</sup> 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.

<sup>193</sup> 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.

<sup>196</sup> 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.

<sup>197</sup> Section 112(2) of the Act.

<sup>198</sup> Section 113(3) of the Act.

<sup>199</sup> Section 112(4) of the Act.

<sup>200</sup> Section 112(3) of the Act.

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
<b>Audit, entry and inspection (Schedule 12)</b>	<b>Service provider</b>	<b>Failure to comply with a requirement of an audit notice</b>	A person commits an offence if they fail without reasonable excuse to comply with a requirement of an audit notice. <sup>201</sup>	<ul style="list-style-type: none"> <li>• Fine<sup>202</sup></li> <li>• Court order requiring compliance with a requirement of an audit notice.<sup>203</sup></li> </ul>
		<b>Knowingly or recklessly providing false information</b>	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. <sup>204</sup>	<ul style="list-style-type: none"> <li>• Fine<sup>205</sup></li> <li>• Imprisonment<sup>206</sup></li> <li>• Court order requiring the person to comply with a requirement of the audit notice or Entry and Inspection Notice.<sup>207</sup></li> </ul>
		<b>Suppressing, destroying or altering information or documents</b>	A person commits an offence if, following an Entry and Inspection Notice, or an audit notice, they: <ul style="list-style-type: none"> <li>a. suppress, destroy or alter, or cause or permit the suppression, destruction or alteration of, information or documents that Ofcom has required; and</li> <li>b. their intention was to prevent Ofcom from being provided with the information or document in its original form.<sup>208</sup></li> </ul>	

<sup>201</sup> Section 111(1) of the Act.

<sup>202</sup> Section 113(1) of the Act.

<sup>203</sup> Section 111(6) of the Act.

<sup>204</sup> Section 111(2) of the Act.

<sup>205</sup> Section 113(2) of the Act.

<sup>206</sup> Section 113(2) of the Act.

<sup>207</sup> Section 111(6) of the Act.

<sup>208</sup> Section 111(3) of the Act.



Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
	<b>A person (including individual on the premises or occupier of the premises)</b>	<b>Intentionally instructing a person acting under Schedule 12</b>	A person commits an offence if they <sup>193</sup> intentionally obstruct a person acting under Schedule 12 (audit, entry and inspection). <sup>209</sup>	<ul style="list-style-type: none"> <li>• Imprisonment<sup>210</sup></li> <li>• Fine<sup>211</sup></li> </ul>
		<b>Failure to comply with a requirement imposed by a person acting under Schedule 12</b>	A person commits an offence if they fail, without reasonable excuse, to comply with any requirement imposed by a person acting under Schedule 12. <sup>212</sup>	
		<b>Providing false information to a person acting under Schedule 12</b>	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. <sup>213</sup>	

<sup>209</sup> 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.

<sup>210</sup> Paragraph 18(2) of Schedule 12 to the Act.

<sup>211</sup> Paragraph 18(2) of Schedule 12 to the Act.

<sup>212</sup> 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.

<sup>213</sup> 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).

Relevant Power	Who is liable?	Offence Summary	Full description of the offence	Penalty
Various	Corporate officers of corporate providers of regulated services	Liability of corporate officers for offences committed by corporate providers of regulated services	<p>Where the provider of a regulated service is a legal person<sup>214</sup> and commits an offence, and it is proved that the offence:</p> <ul style="list-style-type: none"> <li>a. was committed with the consent or connivance of an officer of the provider, or</li> <li>b. is attributable to any neglect on the part of an officer of the entity;</li> </ul> <p>the officer (as well as the entity) commits the offence and is liable to be proceeded against and punished accordingly.<sup>215</sup></p>	Various (depending on the offence committed).

---

<sup>214</sup> Under the law under which it is formed: see section 202(1)(b) of the Act.

<sup>215</sup> 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).