

# Online Safety Transparency Reporting

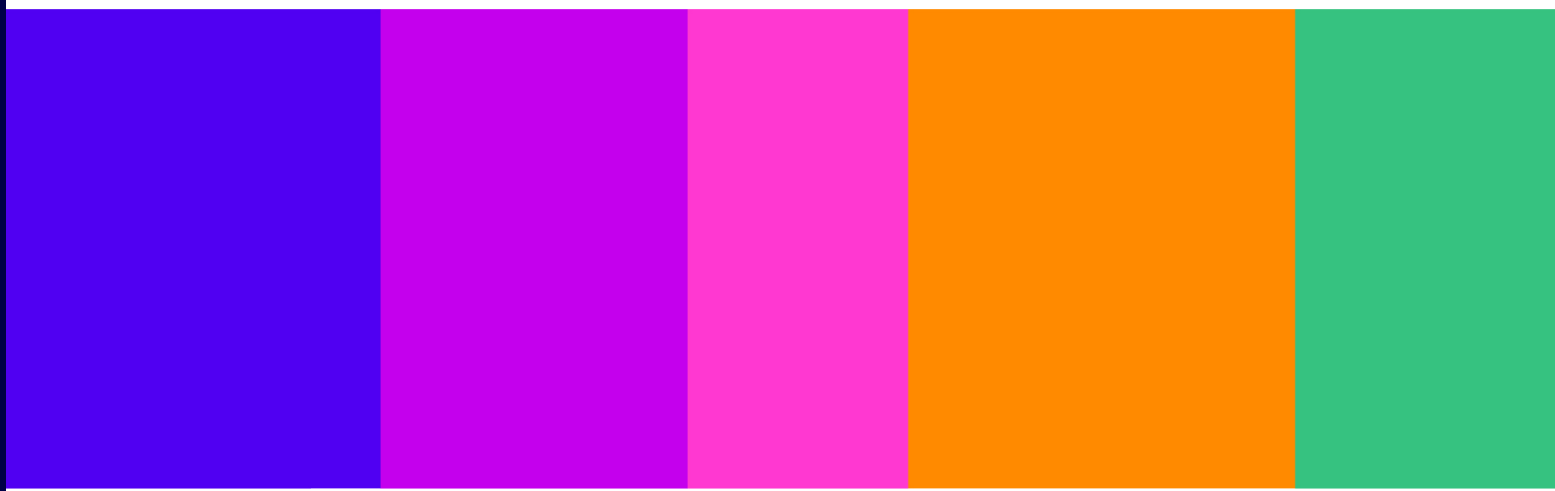
---

## Annex A: Transparency Guidance

**DRAFT for Consultation**

Published 26 July 2024

Closing date for responses: 4 October 2024



# Contents

---

## Section

1. Overview.....	3
2. Background.....	4
3. How Ofcom determinines what transparency reports should cover: principles and factors .....	6
4. How Ofcom determines what transparency reports should cover: engagement .....	13
5. How information from providers' transparency reports will be used to produce Ofcom's transparency reports .....	16
6. Compliance.....	20

## Annex

A1. Matters about which information may be required .....	22
---	----

# 1. Overview

## Introduction

---

**Ofcom is the United Kingdom's (UK) communications regulator, overseeing sectors including telecommunications, post, broadcast TV, radio, and online services. We were appointed the online safety regulator under the Online Safety Act 2023 ("the Act") in October 2023.**

- 1.1 All online services within scope of the Online Safety regime must protect all UK users from illegal content and, where applicable, protect children from online harm. In addition, a small proportion of these services will be categorised and designated as category 1, 2A or 2B services if they meet certain thresholds set out in secondary legislation by Government
- 1.2 Providers of categorised services will be required to comply with a range of additional requirements, largely focused on bringing an appropriate level of safety, transparency, and accountability to the online world, reflecting the nature of such services.
- 1.3 For transparency, providers will be required to publish annual transparency reports based on requirements that Ofcom will issue to service providers by notice. Ofcom must publish its own transparency report summarising industry trends and setting out good practice based on service transparency reports and any additional information, such as new research, to help contextualise those findings for the public.

## Summary of the information in this document

---

- 1.4 Ofcom is required by the Act to produce guidance about the transparency reporting framework.<sup>1</sup> This guidance document has been produced pursuant to that duty. Among other things, it will address:
  - a) Ofcom's approach to transparency reporting;
  - b) how Ofcom will determine what information service providers should include in their transparency reports, including details about the principles and factors Ofcom will consider when deciding what should be included;
  - c) how Ofcom will engage with service providers throughout each reporting cycle;
  - d) how the information in services' transparency reports will be used to produce Ofcom's own transparency reports; and
  - e) how providers are expected to comply with their duties in respect of transparency reporting.

---

<sup>1</sup> Section 78(1) of the Act.

# 2. Background

## Legal Framework

---

### Categorised services

- 2.1 The duty to publish transparency reports only applies to those regulated services<sup>2</sup> that are at that time published on the register of categorised services.<sup>3</sup>
- 2.2 This register, published and maintained by Ofcom, comprises three parts:
- a) one part for regulated user-to-user services meeting the Category 1 threshold conditions;
  - b) one part for regulated search services and combined services meeting the Category 2A threshold conditions;
  - c) one part for regulated user-to-user services meeting the Category 2B threshold conditions.<sup>4</sup>

### Duty to produce report in accordance with Ofcom's notice

- 2.3 Where a service appears on the register (whatever its category) the provider of that service will be liable to produce transparency reports in respect of that service. Once a year, Ofcom must issue every such provider with a notice ("a transparency notice") requiring them to produce a report about that service ("a transparency report").<sup>5</sup>
- 2.4 Each transparency notice must detail a series of requirements. Specifically, Ofcom will set out: the information to be included in the provider's transparency report, the format the information should take, and the date by which the report must be both submitted to Ofcom and published.
- 2.5 Where a provider receives such a transparency notice, it must produce a transparency report in accordance with the terms of that notice, ensuring the information is complete and accurate in all material aspects.<sup>6</sup>

### Information Ofcom may require a provider to produce

- 2.6 The information that Ofcom may require a provider to publish in its report will depend on the category of the relevant service and the type of service. In particular:
- a) Ofcom will only require providers of Category 1 and 2B services to produce "user-to-user information" in their transparency reports. This means information about one or

---

<sup>2</sup> A regulated service includes a user-to-user service or search service that has links with the United Kingdom and is not otherwise exempt by the Act. A regulated user-to-user service can be a combined service, if it includes a public search engine. See Part 2 of the Act for more on these key definitions.

<sup>3</sup> See section 95(2) of the Act.

<sup>4</sup> The threshold conditions are the conditions set out in secondary legislation by Government in accordance with Schedule 11 to the Act.

<sup>5</sup> Where a provider is a provider of more than one categorised service, a notice must be given to the provider in respect of each categorised service (see Section 77(2) of the Act)

<sup>6</sup> Section 77(3) of the Act.

more of the matters in Part 1 of Schedule 8 to the Act provided it relates to the user-to-user part of the service.<sup>7</sup>

- b) Ofcom may only require providers of Category 2A services to produce “search engine information” in the transparency report.<sup>8</sup> This means information about one or more of the matters in Part 2 of Schedule 8 to the Act, providing it relates to the search engine of the service; and
- c) where the service is a combined service, special rules apply depending on the parts of the register that it falls.<sup>9</sup>

2.7 The list of matters referred to above (listed in Schedule 8 to the Act) is broad and covers a range of subjects relating to online safety and the provisions of the Act. The list of matters can be found in the [Annex](#) to this guidance. This guidance sets out detail about how Ofcom determines what information to require providers to report on annually. More information on this can be found in the following chapter.

### Factors that Ofcom must take into account

2.8 In respect of each transparency notice it issues, Ofcom is required to consider the following:

- a) the kind of service it is;
- b) the functionalities of the service;
- c) the number of users of the service;
- d) the capacity of the provider;
- e) the duties set out in Chapter 2 or 3 of Part 3 <sup>10</sup> or Chapters 1 to 4 of Part 4 <sup>11</sup> that apply in relation to the service;
- f) the proportion of users of the service who are children.

### Ofcom’s transparency report

2.9 Separately, Ofcom must also produce and publish its own transparency report at least once a year summarising insights and conclusions drawn from the transparency reports produced by providers. This must include identified patterns and trends, good industry practice and also include additional information Ofcom considers relevant, such as new research, to help contextualise those findings for the public.<sup>12</sup>

2.10 When publishing this, Ofcom must have regard to the need to exclude from publication, so far as it is practicable, any matters which are confidential in accordance with 164(3) and (4) of the Act.

---

<sup>7</sup> For the definition of “user-to-user part (of a service)” see section 236 of the Act.

<sup>8</sup> For the definition of “search engine” see section 229 of the Act.

<sup>9</sup> If a combined service is provided that is both a Category 2A service and a Category 1 or 2B service, Ofcom may require the production of user-to-user information or search engine information or both. However, if a combined service is provided that is only a Category 2A service and not a Category 1 or 2B service, then Ofcom may only require the production of search engine information.

<sup>10</sup> The duties of care that user-to-user and search services must comply with set out in Schedule 8, part 3 of the Act. These duties of care include, but are not limited to, carrying out illegal content and children’s risk assessments, protecting children’s online safety, empowering adult users, protecting content of democratic importance, and duties about content reporting and complaint processes.

<sup>11</sup> These are the additional duties service providers must comply with. These duties include, but are not limited to, user identity verification, reporting child sexual exploitation and abuse content, terms of service duties and deceased child user duties.

<sup>12</sup> Section 159 (1-5) of the Act

# 3. How Ofcom determines what transparency reports should cover: principles and factors

- 3.1 In this chapter we explain how we will use key principles to determine the information in a transparency notice.
- 3.2 We will always endeavour to engage with providers before we formally issue a transparency notice, so there are opportunities to ask questions about its contents or the process more generally. It is therefore important that providers understand our decision-making process so that they can make the most of that engagement process (which we discuss in more detail in the next chapter).

## What we can require in reports: illustrative examples

- 3.3 As discussed in the previous chapter, the matters that Ofcom can require a user-to-user or search service to produce in its transparency report are listed in Schedule 8 to the Act. The Schedule covers a wide variety of matters relating to online safety, including in relation to the service itself (regarding its systems and processes, design, operation and user base), the incidence of regulated content on the service, and the safety measures adopted for the purpose of complying with certain duties in the Act, among other things. For ease of reference, we have reproduced the matters from Schedule 8 in the [Annex](#) to this Guidance.
- 3.4 In the table below, we set out a few illustrative examples of the information that we might request in our notices from user-to-user and search services by reference to some of the matters listed in Schedule 8.

Matter	Examples of types of information
<b>The incidence of illegal content, content that is harmful to children, relevant content and content to which section 15(2) applies on a service.<sup>13</sup></b>	We may require information about how often content appears on a user-to-user service that is illegal or harmful to children. For instance, in existing industry transparency reports, some services report a variety of metrics relating to incidence for content that violates the terms of service, which together help build a picture of the availability of this content on the service and how it is tackled.
<b>The incidence of illegal search content and search content that is harmful to children on a service.</b>	We may require information about how often search content that is illegal or harmful to children appears on a search service.

---

<sup>13</sup> Section 15(2) is a duty to include in a service features which adult users may use or apply if they wish to increase their control over content. This includes features that reduce the likelihood of the user encountering content or alert the user to content present on the service that is a particular kind of content.

Matter	Examples of types of information
<p><b>The dissemination of illegal content, content that is harmful to children, relevant content and content to which section 15(2) applies by means of a service.</b></p>	<p>We may ask about functionalities or systems on a service that affect the dissemination of harmful content, such as the speed or breadth with which harmful content is shared on the service before being removed, or the speed of enforcement action. For instance, some services report on average time taken for a piece of content to be reviewed and/or enforced after it received a user report.</p> <p>We may also require information that helps us understand the risks of cumulative harm to children as a result of being repeatedly exposed to harmful content. An example of this could be the average number of individual pieces of content that are harmful to children encountered by each unique user/account within an agreed time period.</p>
<p><b>The number of users who are assumed to have encountered illegal content, content that is harmful to children, relevant content or content to which section 15(2) applies by means of the service</b></p>	<p>We may require information about how many users have been exposed to harmful content in a given period. For example, in existing industry transparency reports, some services use ‘prevalence’ or ‘violative view rate’ to show the percentage of views on the service which were of content that violates policies.</p>
<p><b>The systems and processes that a provider operates—</b>  <b>(a) to direct users of the service to information about how they can protect themselves from harm in relation to illegal content and content that is harmful to children, and</b>  <b>(b) to counteract or provide support to users of the service in relation to illegal content and content that is harmful to children present on the service.</b></p>	<p>We may ask for information that tells us about how users engage with informational pages about safety measures. For instance, we might ask for the frequency of UK user visits to informational pages such as terms of service, transparency reports or user policies.</p> <p>We may ask for information that tells us how effective user reporting tools are for supporting users against harmful content they may encounter on a service.</p> <p>We may also require information that tells us about the accuracy of systems and processes for identifying content that is illegal or harmful to children. For instance, the proportion of content that was incorrectly identified as violative of terms of service. This may tell us about the effectiveness of content moderation systems.</p>
<p><b>Functionalities designed to help users manage risks relating to search content that is harmful to children.</b></p>	<p>We may ask for information that tells us about the functionalities search services offer to users to help manage risks relating to content that is harmful to children, for instance, content that promotes self harm or suicide. This could include information about safety settings for children or tools that enable users to have control over the search results children can view, and the take-up of these tools.</p>

## How we determine what to require in reports

---

### The wider context

- 3.5 Ofcom has identified four key outcomes that Ofcom expects the overall implementation of the Act to achieve to ensure UK citizens are safer online. We will draw on these to help us prioritise what information we will require each year and for each service in the notices.
- 3.6 To support our mission to ensure people in the UK are safer online, we are committed to an approach that, so far as possible: (i) strengthens safety **governance** in online services, (ii) ensures online services are **designed and operated** with safety in mind, (iii) gives greater **choice** for users so they may have more meaningful control over their online experiences, and (iv) promotes **trust** in services' safety measures.<sup>14</sup>
- 3.7 To drive forward these aims, we will seek to deliver an effective transparency reporting regime that will drive improvements on services and empower UK users with information to live safer lives online. To achieve this in practice, we will need to ensure that through our notices, we are requiring information that is meaningful for our audiences.
- 3.8 We will draw on these four aims to help inform our priority areas for transparency reporting every year: they will direct our focus towards key risks, safety measures or governance practices. They will inform our efforts to shine a light on deficiencies or best practices from industry that can help drive improvements across the sector.

### Our approach: key principles and factors

- 3.9 Our approach for determining what user-to-user information or search engine information we will require each year, and for each service, will be guided by certain key principles. We have identified these principles as important building blocks for delivering our transparency powers effectively.
- 3.10 First, we want to ensure that the information we request is not only **relevant** to the service(s) in question, but also **appropriate** to ask for in the circumstances having regard to our strategic priorities. Our overall intention is for the reports produced by categorised services to be sufficiently tailored to ensure that they reflect the way in which each service is designed, used and operated, whilst also being sufficiently standardised to allow for meaningful comparison in certain areas.
- 3.11 Second, as with all our work, we will look to act **proportionately** in our decision-making. In each case, we will only consider requesting information that is necessary for the purpose of helping us meet our aims and policy objectives. We also recognise that providers record information in different ways, and face different challenges in producing it to fit certain specifications, so will take steps to ensure that the requirements are not unduly onerous.
- 3.12 In applying these principles, we will always take account of at least the following factors, reflecting the requirements in paragraph 37 of Schedule 8 to the Act<sup>15</sup>:
- a) the kind of service;

---

<sup>14</sup> See Figure 1, [Roadmap in Ofcom's approach to implementing the Online Safety Act](#) - Ofcom

<sup>15</sup> See Chapter 2 for full discussion of the legal framework; in Annex 1 we reproduce the matters detailed in Schedule 8 for ease of reference.



- b) the functionalities of the service;
  - c) the number of users of the service;
  - d) the capacity of the provider;
  - e) the duties set out in Chapter 2 or 3 of Part 3, or Chapters 1 to 4 of Part 4 that apply in relation to the service (“the relevant duties”);
  - f) the proportion of users of the service who are children.
- 3.13 While we may place more or less weight on any of these factors in a given case, none of the above takes precedence over others listed; we will look to consider them holistically. The discussion below explores how we will consider these factors and apply the principles discussed above.
- 3.14 **The kind of service.** To ensure that our assessment leads to requests that are appropriately tailored, we will consider whether the service is of a kind that gives rise to particular risks. Our understanding of the specific risks associated with a given kind of service will help us to narrow the topics of information that we require providers to report on. We will typically seek to prioritise requesting information about risks that are most evidently generated by the kind of service in question. One source of information that we will draw on is Ofcom’s risk profiles.<sup>16</sup> The risk profiles are lists of risk factors that providers may consider for the purposes of conducting their own risk assessments.<sup>17</sup> Service type is one of the factors considered in the risk profiles. However, we will also call on other sources of evidence about the relationship between the kind of service and risk of harm to inform our process. This might include third-party research, Ofcom research, or information published by services themselves. It could also include information from providers’ own risk assessments, where available. By way of example, Ofcom’s draft risk profiles presently consider the provision of “messaging services” as a risk factor for high severity harms such as CSEA, grooming and terrorism due to the nature of that service type<sup>18</sup>. In considering what information we require a messaging service to produce in its transparency report, we would therefore prioritise information about the risk of these kinds of harms and relevant safety systems and processes.
- 3.15 **Functionalities of the service.** We will adopt a similar approach regarding the functionalities of the service. To understand how functionalities might affect risk, we will typically use findings from Ofcom’s registers of risk (for illegal offences and for content harmful to children), the associated risk profiles and available research, including Ofcom’s own and third-party studies. These findings will inform our understanding of how the functionalities on a given service generate certain risks, either independently or in combination with other factors, and guide our decision-making when we come to making requests in our notices. Generally, where we know that the functionalities on a given service are likely to generate specific risks of harm, we will prioritise asking for information about those issues, as well as any safety measures that might be particularly relevant to those issues. For example, Ofcom’s risk profiles consider livestreaming functionality as a risk factor for harms derived from specific terrorism offences. For a service that provides livestreaming as one of its many functionalities, we may therefore prioritise seeking information about the safety systems

---

<sup>16</sup> Note that references to different “kinds” of service (such as this) include references to services grouped together for this purpose in Ofcom’s risk profiles: see section 236(4) of the Act.

<sup>17</sup> See Appendix A of Ofcom’s illegal harms [Service Risk Assessment Guidance](#).

<sup>18</sup> See Appendix A of Ofcom’s illegal harms [Service Risk Assessment Guidance](#).

that service has in place for livestreaming and the effectiveness of those systems in mitigating the related risks.

- 3.16 **The number of users on a service.** Ofcom will consider the evidence available to us to understand how the number of users on a service might affect the nature of risks posed by the service. First, we will seek to understand how the size of the user base interacts with other features, including the functionalities of the service, to affect risk. Based on this, we will tailor our requirements to prioritise information about risks that may be particularly prevalent based on the size and characteristics of the service.
- 3.17 Second, we recognise that the safety systems that providers put in place for the purposes of making their services safer may differ considerably on account of having either a particularly large or particularly small user base. For instance, a service with a relatively large user base may rely more regularly on automated systems for risk detection and risk mitigation due to the scale of user-generated content present on the service. We will generally look to ensure that the requests we make about safety systems and processes are relevant to the size of the service’s user base.
- 3.18 Third, we will have regard to changes in the size of the service’s user base over time. This will allow us to identify services that have a quickly expanding user base in the UK. Ofcom’s draft assessment of risks of illegal harm found that, “[a] fast-growing user base may negatively affect a service’s ability to moderate effectively, given the increased scale and sophistication of the moderation technologies and processes required to keep track of a fast-growing user base (particularly since the sources of risk, and kinds of harms on the service, can change quickly as the user base develops)”.<sup>19</sup> Therefore, where we identify such services, we may include requirements in their notices to generate information about their governance systems and the safety measures that they have in place to protect their increasing number of UK users.
- 3.19 **The proportion of users of the service that are children.** We will take into account how the proportion of users that are children on a service might require us to tailor our information requirements. We will draw on various sources to understand where children in the UK are spending their time online, including the results of providers’ Child Access Assessments, Ofcom’s evidence base and external research. We may also consider information about how children interact with the services that they use to further refine any questions that we ask about the measures that services have in place to protect children. For services that have any child users on their service, we may ask questions specific to children, including any specific risks relevant to children, measures in place on the service to protect children and information that demonstrates how effective those measures are. Where a service has a significant proportion of children on their service, our transparency notices will typically require services to publish information about how they keep children safe, including detailed and specific information about relevant risks and safety measures.
- 3.20 **The relevant duties.** We will always take account of the relevant duties that apply to the service, specifically those falling within Chapter 2 or 3 of Part 3 or Chapters 1 to 4 of Part 4 of the Act. Broadly, the duties in Part 3 cover the illegal content safety duties (including those that target services likely to be accessed by children). These apply to all user-to-user services and search services respectively. Chapter 2 of Part 3 contains some additional duties that

---

<sup>19</sup> [Volume 2: The causes and impacts of online harm – Ofcom](#), 2023, p.321.

apply in respect of Category 1 services. Similarly, Chapters 1 to 4 of Part 4 cover a series of other duties that apply in respect of certain categorised services.<sup>20</sup>

- 3.21 In deciding what to request through transparency notices, we will be particularly mindful of the category within which a service falls and the duties that apply to the service as a consequence. In our notices, we will not ask services to publish information about duties that it is not required to comply with. We recognise that, in some cases, services may be categorised or de-categorised during the reporting year (and that additional duties may apply for different periods of time). Where we ask for information or data relating to how a service is complying with such additional duties, we will only ask services to produce information about duties that the service must comply with at the time we issue the notice.
- 3.22 Our consideration of the duties of the service also concerns whether the service is required to comply with the protection of children duties. We do not expect to ask services to report information about risks of content that might be harmful to children if they are not subject to the protection of children safety duties, nor specific measures intended to mitigate these kinds of risks. Where relevant, we may ask these services about the processes that they have in place to prevent children from accessing their services. All services are required to comply with illegal safety duties, so we will always retain the option to ask for information about how services are complying with these duties through our transparency notices.
- 3.23 **The capacity of the service provider.** In principle, we expect providers to have resources at their disposal to fulfil their transparency duties in a timely fashion. We do not anticipate that the absence of capacity on behalf of a provider as being determinative of how we choose to frame our requests, particularly where the subject matter may be regarded as routine or typical in the circumstances. However, we recognise that cases may differ, and we will engage with providers during the draft notice process, discussed in the following chapter, to allow the opportunity for representations about the likely time, cost and effort to give effect to the proposals in the draft notices.
- 3.24 When considering capacity, we are principally (though not exclusively) concerned with the providers' financial resources and the level of technical expertise available, or which it is reasonable to expect would be available to the provider given its size and financial resources.<sup>21</sup>

### Other factors that will affect the design of transparency notices

- 3.25 Beyond the factors set out in the Act, there are two other factors that will affect the requirements included in transparency notices.
- 3.26 The **first** is Ofcom's consideration of whether the information has already been provided or published by the service. We will take note of the information that services already include in their voluntary transparency reports and published reports required under other regulatory regimes. This may be used to inform considerations of what information is feasible for services to collect and where it may be useful to require UK-specific versions of data that has already been published.
- 3.27 The **second** is our consideration of how we can best use our powers to reveal patterns or trends derived from service transparency reports, with a focus on whether some information should be reported consistently over time and/or across the industry. We are required to

---

<sup>20</sup> The exception is Chapter 2 which relates to the reporting of CSEA content (and which applies more widely).

<sup>21</sup> See section 236(1) of the Act (definition of "capacity").

summarise important patterns or trends that we have identified in our own transparency report, which will draw upon this information. More information on this process is outlined in Chapter 5.

- 3.28 An important component of the decisions we make about our notices will therefore be whether we will require certain pieces of information to be reported consistently over time – what we are calling ‘**core**’ information requirements – or on a one-off basis, which might support our ability to establish patterns across the industry, but not across time.
- 3.29 The consistent reporting of information over time can support our efforts to provide users and the UK public with analysis of trends in industry safety performance. For instance, to shed light on the impact of dissemination of harmful content on users of a service, we may ask for information about the number of users that are likely to have encountered harmful content in consecutive notices. The publication of these metrics in continuous transparency cycles would allow Ofcom and other readers of the reports to reflect on changes in users’ exposure to risk over time and therefore to consider the potential reasons for such changes.
- 3.30 Not all information that we ask services to publish in a notice will be “**core**” information. In our efforts to assess safety trends, we will seek to analyse trends across the industry as well as across time. To do this, there may also be some information that we wish to ask about on an ad-hoc basis: a “**thematic**” set of information requirements that focus on areas that Ofcom has identified based on its areas of regulatory focus each year. We may, for instance, seek to prioritise information around specific priority illegal harms for one reporting year, and the protection of children in another. An example of thematic information requirements would be a focus on the efficacy of measures to address specific manifestations of CSAM across relevant services. We may ask for detailed information about the governance processes, internal KPIs or safety measure outcomes relating to this topic. Our consideration of services’ functionalities and service type would help us to identify which services do and do not generate risks of CSAM and would therefore receive these additional information requirements. These thematic requirements will enable Ofcom to compare different industry efforts on specific topics, whether a priority area of risk or a certain type of safety measure. We may also identify priority topics for focus based on extraneous or topical events, such as UK elections or terror incidents, that may warrant reporting.
- 3.31 Focus areas may change annually and the information we require will be tailored to individual services and may differ in scope and scale. We will apply our principles and factors set out above when considering if we will require more detailed and specific information from some services over others. Depending on the focus area, some providers may be excluded from thematic reporting requirements in a given year if the focus area is not relevant to their service. We may require information on the specific focus area for just one reporting year, or several, depending on the specific nature of the topic and the information produced.
- 3.32 In addition to considering the value of information reported ad hoc or across time, we will also assess where there may be opportunities to ask for the same information across multiple services. Rather than enabling comparison over time, this kind of information would enable **comparisons across the industry**. When we decide what information to require of services each year, we will therefore consider if it is possible to do so in a way that produces comparable information from different services or if that information needs to be **bespoke to the specific service** in order to remain appropriate and relevant.
- 3.33 Once we have settled on the substance and form of our requests, we will issue the provider with the draft notice(s) accordingly.

## 4. How Ofcom determines what transparency reports should cover: engagement

- 4.1 In this Chapter, we explain how Ofcom will deal with providers of services prior to issuing a formal transparency notice. We consider that timely and constructive engagement on these matters is essential to ensuring that the transparency reporting regime operates effectively.

### Our approach

---

- 4.2 Ofcom will endeavour to engage with providers during each transparency reporting cycle to inform decisions about information requirements and improve providers' understanding of the transparency reporting regime. While we aim to be consistent about when and why we engage with providers, we may pursue different types of activities depending on the nature and depth of the discussion, whilst ensuring all providers are treated equally. For example, we may offer in-person meetings to providers that have been newly categorised to ensure that they understand the full scope of their duties. For providers whose service/s have been categorised for some time, we may use lighter-touch modes of communication, including email correspondence.
- 4.3 There are some engagement activities that we plan to carry out in respect of each annual reporting cycle. In particular, before we formally give a provider a transparency notice, we will first issue it to them in draft form to allow the opportunity for representations to be made in respect of its requirements. We discuss more about the nature and purpose of this engagement below from paragraph 4.7.
- 4.4 As the transparency regime evolves, Ofcom will gather evidence about what types of transparency information are the most valuable for improving user safety in the UK. As our understanding develops, we will seek to build consistency into the design of transparency notices, where possible.
- 4.5 In cases where Ofcom does not know enough about how a particular service operates to inform our decisions about the contents of our notices, we may consider additional engagement to gather such information. Where appropriate, this might include the use of our statutory information gathering powers or voluntary engagement activities, such as publishing Calls for Input (CFIs) to seek input about the suitability of certain metrics.

## Transparency notices: the engagement process

---

- 4.6 Once published, the register of categorised services will be updated at appropriate intervals, and this may result in Ofcom adding or removing services from the public register. Ofcom may contact providers that have been newly categorised, including for the first time, to ensure we have the relevant contact details required for issuing their first transparency notice.
- 4.7 Each year Ofcom will share with providers a draft transparency notice (or, where the provider provides more than one categorised service, drafts of the transparency notices), containing the information Ofcom proposes to require services to produce in their transparency reports. This will offer the opportunity for providers to make written representations on the proposed information to be produced within the report before the notice is formally issued. Among other things, this process is intended to ensure the requests are clear, targeted and proportionate to the technical capabilities and capacity of the provider.
- 4.8 The process of issuing the draft notices through to final notices will be administered with the assistance of Ofcom's Information Registry ('the Registry')<sup>22</sup>. The Registry supports project teams across Ofcom in issuing and coordinating information requests and responses. The process for issuing notices can be understood broadly as three steps:

### Step 1 – Ofcom shares a draft notice

- 4.9 Prior to formally exercising its powers to issue a notice under the Act each year, Ofcom will send draft transparency notices to providers. Timings for this may differ between reporting periods and services, depending on various factors such as how we choose to stagger the notices, and the level of engagement that is required. The draft notice will set out Ofcom's proposals for the information required, the format that the information needs to be published in, the date the report should be submitted and published, and any other information about the matter of its publication.

### Step 2 – Providers may make written representations in respect of the draft

- 4.10 Providers may make evidence-based written representations in respect of the information that we propose to require to be included in the report or the manner and format in which that information is required. Additionally, the provider may ask for clarifications on the information required. The draft notice will contain details on how providers should make their written representations.
- 4.11 Ofcom will expect to receive representations by the deadline set in the draft notice. We will have regard to all representations in the preparation of the final notice.

### Step 3 – Ofcom formally issues the notice

- 4.12 We will formally issue the provider with their transparency notice after the representations process is completed. Once the notice has been formally issued, we do not expect to engage further with providers about the transparency notices or the contents of their report, because all such issues should have been resolved through the draft notice process. If we decide to make material changes to the final notice from the draft notice, we will include a covering letter outlining what changes we have made. Ofcom may in certain circumstances decide to liaise with providers following the issuing of the final notice, for example for

---

<sup>22</sup> <https://www.ofcom.org.uk/about-ofcom/what-we-do/information-registry/>

necessary clarifications or urgent extension requests. However, such engagement will be considered only where necessary and, on a case-by-case basis.

- 4.13 The notices will be served on persons who are providers of the relevant regulated service(s) in accordance with the service requirements set out in the Act.<sup>23</sup>

### Confidentiality and commercial sensitivity

- 4.14 Ofcom may require information to be produced in a report in respect of a service that provider considers commercially sensitive or confidential for other reasons. Before deciding on whether to require such information to be published, Ofcom will provide an opportunity during the draft notice process to the provider to present any concerns arising out of such publication, including around the confidentiality of the information, and will seek to take this into account when reaching a decision. When considering any concerns, we will typically have to balance the provider's concerns around publication, including possible harm to legitimate business interests, against the extent to which publication of the information is necessary to exercise our functions around transparency. In some cases, we may consider alternatives to our requested information, where appropriate, if the alternative information is sufficient, reasonable and meets our aims.
- 4.15 In some cases, service providers may have submitted information to Ofcom that has not been formally requested and that is not intended for publication and may be considered by them as confidential. Ofcom is prohibited from disclosing information received from a business unless we receive consent from the relevant business or can justify the disclosure under section 393(2) of the Communications Act 2003. Therefore, if Ofcom were considering the disclosure of such information, we may engage directly with the relevant service provider about the proposed disclosure.<sup>24</sup>

---

<sup>23</sup> Section 208(1)-(2) of the Act

<sup>24</sup> Section 393(2) of the Communications Act



# 5. How information from providers' transparency reports will be used to produce Ofcom's transparency reports

- 5.1 This Chapter sets out detail about the transparency report that Ofcom must produce each year, which must be based on the information in providers' transparency reports. This will always include a summary of conclusions drawn from provider transparency reports regarding any patterns or trends which we have identified as important to share along with a summary of measures which we consider to be good practice (but may cover other things too).<sup>25</sup>

## Our approach

---

### What we plan to achieve

- 5.2 While provider transparency reports will typically offer insight into how individual services address risks and mitigate harms on their services, Ofcom's transparency reports will contextualise those findings, drawing out points of comparison between services and highlighting examples of best and poor practice for the wider industry.
- 5.3 In summarising patterns and trends in Ofcom's annual transparency reports, including industry best practice, we will seek to meet two ambitions. The first is to encourage services to improve their safety systems and processes. We will hold services to account by commenting on gaps in their systems and processes and enable learning from practices across the wider industry. The second is to empower UK users with relevant and accurate information about risks and safety outcomes on services so that they can take informed decisions about how to live their lives online.

### How we will get there

- 5.4 In putting together Ofcom's transparency reports, we want to provide the general public and industry with information that is comprehensive, informative, and accessible. To deliver this, we focus on the following areas.
- 5.5 **Converting data into insight:** Ofcom's reports will translate technical information in provider reports into accessible insights for users. Such insights will highlight the implications of reported data about risks and safety outcomes, so that users can make informed choices about the services they use. Once published, we may look to engage with expert organisations (among others) to ensure our report is properly understood and any improvements we can take forward for future reporting.

---

<sup>25</sup> Section 159 of the Act



- 5.6 **Seeking comparability:** We will seek to compare findings from provider reports to understand developments or concerns in trends across the industry. Ofcom's reports will highlight patterns and trends from the information requirements explained in Chapter 3. The types of information published by services (core and thematic, comparable and bespoke - outlined from 3.28 to 3.32) will affect our approach to presenting and communicating our conclusions. Where information is comparable over time and/or across services, we will focus on identifying and presenting patterns and trends in our reports. Where information is not standardised in this way, we will present individual insights and seek to place them in the relevant context. We hope that through comparability, we can incentivise services to pursue self-improvements and demonstrate leadership in the industry around good safety practice on certain issues and areas. We may seek to make comparisons in the following ways within, and between services:
- 5.7 We may seek to compare how individual services are performing **over time**, focusing on specific metrics or qualitative information, and providing commentary on the implications of those changes, or lack of, from one period to the next. This will enable us to identify benchmarks for good practice that are specific and relevant to the service in question. For example, we may monitor harm reduction metrics or changes to staffing. These comparisons would enable us to review service-specific context, considering the drivers of those changes and their implications relative to the size of the services and the level of risk to users. We may also seek to compare a metric or piece of information that has been reported across multiple services, where the same information has been required **across the industry**. Any longitudinal or comparative analysis over time or between services will take into account differences in how individual services report information, including variations in definitions and data collection methodologies.
- 5.8 **Shining a light on best practice and gaps in industry efforts:** We will seek to identify examples of good practice and highlight the different approaches services can take to address various issues related to online safety, and the benefits and limitations of those approaches. By doing this, we hope to support services across the industry, including small and newly created services, to learn from the experiences of other companies. Our analysis will also seek to identify any gaps or deficiencies in industry or specific services' efforts to protect UK users.

## The process

- 5.9 The process for analysing and producing Ofcom’s transparency reports can be understood broadly as these steps outlined in fig 2.

Fig 2.



- 5.10 There will be some information that we choose to report on year on year to show changes or trends over time. This will be drawn from the “core” information requirements that we discuss in chapter three. We will seek to present our findings in a way that enables users to compare the safety actions and outcomes of different services, where possible.
- 5.11 Ofcom’s reports may also assess any “thematic” information published by service providers, as discussed in chapter three. This will enable us to draw out insights and best practices about certain risks or safety measures alongside a more general assessment of industry trends. Ofcom may choose to publish more than one report a year to serve these different purposes.
- 5.12 We will seek to communicate our proposed areas of focus for the year ahead of transparency reporting. This will give providers an idea of what kind of information they may be required to report on, and the issues Ofcom will be looking to shine a light on in its report for that year.
- 5.13 Ofcom will carefully consider the information we include in our annual report(s) and providers reports to ensure alignment with our overarching strategy for transparency reporting for that year. This will ensure that we can optimise the information in provider reports to support the thematic areas of focus in our transparency reports.

## Sources of information for Ofcom's reports

- 5.14 Ofcom will primarily use information from providers' transparency reports to inform its own reports. However, we may also draw on information from other sources. This might include trends, insights, or data from third parties such as academics, independent research organisations and Ofcom's own research.
- 5.15 Ofcom may also draw on information obtained through formal and informal information gathered from providers, including through our statutory powers to issue information notices and through broader engagement with stakeholders. Where such information has been gathered for a different purpose, we will engage with providers on this.
- 5.16 Where we draw on additional data or information sources for the purposes of producing Ofcom's transparency reports, we will ensure the information is accurate and all necessary caveats are clearly stated. For example, we would clearly highlight differences in the methodology used to generate different data sources and the subsequent limits of any comparative analysis or conclusions. Ofcom frequently brings together multiple sources of data in its research and publications. We conduct thorough reviews of all third-party datasets or metrics as well as our own research, assessing the design of the data collection and analysis conducted so that we understand any limitations. We may consider if the research is, for instance: justifiable; appropriate; specific; useful for the stated purpose; replicable; clear about its strengths and limitations; and consistent in method from period to period.
- 5.17 For any information provided to Ofcom in advance of publication of its transparency report that was not included in the providers' transparency report, Ofcom will have regard to the need to exclude from publication confidential matters in accordance with Section 164 of the Act.

# 6.Compliance

- 6.1 Providers are required by the Act to meet the requirements of their transparency notice(s) and produce accurate and complete information in their reports. These duties are enforceable requirements under the Act.<sup>26</sup> In this Chapter, we elaborate on our approach to compliance and enforcement.

## Our approach

---

### What we expect from service providers

- 6.2 Providers of services have a legal duty to produce a transparency report in accordance with the requirements of the notice and must ensure that the information in the report is complete and accurate. This is fundamental for ensuring Ofcom, users, industry, and other audiences of transparency reporting can rely on and make informed decisions from the information provided. Where we are concerned about potential non-compliance with the notice requirements, we will assess the issue in line with our Online Safety Enforcement Guidance<sup>27</sup> and consider whether it is appropriate to take enforcement action in the circumstances.<sup>28</sup>
- 6.3 Ofcom may take enforcement action where a provider has failed to produce a transparency report, in relation to relevant service, or if it fails to:
- a) include information of a kind specified or described in the notice;
  - b) produce the report in the format specified in the notice;
  - c) submit the report to Ofcom by the date specified in the notice; and
  - d) publish the report in the manner and by the date specified in the notice.
- 6.4 Ofcom may also take enforcement action where a provider's transparency report contains information which is not complete and/or accurate in all material respects.
- 6.5 Providers of services are responsible for ensuring the information included in their reports is complete and accurate, in line with their legal duties. Providers should conduct appropriate checks and governance processes to ensure that the report is properly reviewed and interrogated prior to submission to Ofcom and publication. This should include being signed off by an appropriately senior accountable person. Providers should consider the following prior to submission and publication of their reports:
- a) the level of detail they have provided in response to each request;
  - b) whether they have sufficiently addressed all the requests in the notice; and
  - c) the approach taken to quality assure information and data provided.
- 6.6 We are unlikely to accept failures by providers to comply with their duties either because of delays or failures to meet the requirements of our notices for reasons which could have been anticipated and prepared for in advance. For instance, through the engagement we

---

<sup>26</sup> Section 131 of the Act

<sup>27</sup> Ofcom, '[Protecting people from illegal harms online: Annex 11: Enforcement guidance \(draft for consultation\)](#)', (9 November 2023).

<sup>28</sup> Ofcom's enforcement powers are set out in Chapter 6 of Part 7 of the Act and enable us to enforce the duties and requirements applying to service providers and, where relevant, other persons or third parties.

have had with the relevant provider prior to issuing the transparency notice, we expect providers to take the appropriate steps to ensure they have the necessary resource and mechanisms to fulfil their transparency reporting duties in a timely and efficient manner.

- 6.7 If Ofcom is made aware that the information provided may be inaccurate or incomplete, either through our own checks or reported to us by the public, researchers, civil society organisations, journalists, and other audiences of the transparency reports, we may take enforcement action in response.

### Enforcement action by Ofcom

- 6.8 Failure to comply with Ofcom's transparency powers may carry significant consequences and may result in Ofcom taking enforcement action. Our approach to enforcement action for non-compliance with transparency duties will be in line with the Act and our Online Safety Enforcement Guidance,<sup>29</sup> which sets out how we decide whether to take enforcement action, and the processes that we would typically follow.
- 6.9 Where we consider that a service provider may not be meeting its obligations under the Act, we have a variety of tools available to us to drive change and improve compliance. These include opening an investigation and using our statutory powers under the Act to investigate whether a service provider has contravened its obligations and take a decision to that effect. In addition to these statutory powers, Ofcom also has a range of non-statutory tools which we may use in response to a potential compliance concern instead of opening an investigation. Ofcom's Online Safety Enforcement Guidance provides more information on the action we can take should services fail to comply with their transparency duties.
- 6.10 Ofcom may take separate enforcement action in relation to one or more failures to comply with such a requirement(s) with powers to impose a penalty where it finds non-compliance. A penalty can be up to 10% of qualifying worldwide revenue or £18 million (whichever is greater).<sup>30</sup> We can also require the provider to take steps to comply with the transparency duties or remedy the failure to comply with that duty. When taking enforcement action for non-compliance of such requirements, we will enforce in line with the Act and with our Online Safety Enforcement Guidance.
- 6.11 Where Ofcom takes enforcement action against a provider of a regulated service, these measures may, in certain circumstances, also be applied to any other entity related to the provider of the service or an individual controlling the provider of the service<sup>31</sup>.

---

<sup>29</sup> Our draft [Online Safety Enforcement Guidelines](#) provide further information about the circumstances in which enforcement action may be applied to related entities.

<sup>30</sup> Penalties will be determined and set in accordance with our Penalty Guidelines and will consider all the circumstances of the case and will take into account the potentially relevant factors set out in the Penalty Guidelines - [penalty-guidelines-september-2017.pdf \(ofcom.org.uk\)](#).

<sup>31</sup> Schedule 15 of the Act gives Ofcom powers to issue notices that may hold companies and individuals jointly and severally liable for a contravention. Our draft [Online Safety Enforcement Guidelines](#) provide further information about the circumstances in which enforcement action may be applied to related entities.

# A1. Matters about which information may be required

This Annex contains the matters about which information may be required listed in Schedule 8 of the Act which outlines the broad range of information we can require about online safety matters from user-to-user services (Part 1) and search services (Part 2).<sup>32</sup>

## Part 1. Matters about which information may be required: user-to-user part of service

---

1. The incidence of illegal content, content that is harmful to children, relevant content and content to which section 15(2) applies on a service.
2. The dissemination of illegal content, content that is harmful to children, relevant content and content to which section 15(2) applies by means of a service.
3. The number of users who are assumed to have encountered illegal content, content that is harmful to children, relevant content or content to which section 15(2) applies by means of the service.
4. The formulation, development, scope and application of the terms of service.
5. The systems and processes for users to report content which they consider to be illegal content, content that is harmful to children or relevant content.
6. The systems and processes that a provider operates to deal with illegal content, content that is harmful to children and relevant content, including systems and processes for identifying such content and taking it down.
7. Functionalities designed to help users manage risks relating to content that is harmful to children and relevant content.
8. Features, including functionalities, that a provider considers may contribute to risks of harm to individuals using the service, and measures taken or in use by the provider to mitigate and manage those risks.
9. The design and operation of algorithms which affect the display, promotion, restriction or recommendation of illegal content, content that is harmful to children, relevant content or content to which section 15(2) applies.
10. Measures taken or in use by a provider to comply with any duty set out in Chapter 2 or 4 of Part 3 or section 38 (including in particular measures that are described in a code of practice under section 41).
11. Measures taken or in use by a provider to comply with the duty set out in section 64(1) (user identity verification).

---

<sup>32</sup> Schedule 8, Part 1 and 2 in the Act.

12. Arrangements that a provider has in place for the reporting (in the United Kingdom or elsewhere) of content relating to child sexual exploitation and abuse, and measures taken or in use by a provider to comply with a requirement under section 66.
13. Measures taken or in use by a provider to comply with any duty set out in section 71 or 72 (terms of service).
14. Measures taken or in use by a provider to comply with any duty set out in section 75 (deceased child users).
15. The systems and processes by which a provider assesses the risk of harm to individuals from the presence of illegal content or content that is harmful to children—
  - a) when the service is initially being designed or developed,
  - b) when any further development or update to the service is being considered, and
  - c) while the service is in operation.
16. The systems and processes that a provider operates—
  - a) to direct users of the service to information about how they can protect themselves from harm in relation to illegal content and content that is harmful to children, and
  - b) to counteract or provide support to users of the service in relation to illegal content and content that is harmful to children present on the service.
17. Co-operation by a provider with government, regulatory or other public sector bodies in the United Kingdom, in particular those involved in the enforcement of the criminal law.
18. Measures taken or in use by a provider to provide for a higher standard of protection for children than for adults.
19. Measures taken or in use by a provider to improve the media literacy of users, and an evaluation of the effectiveness of such measures.
20. Any other measures taken or in use by a provider which relate to online safety matters.

## Part 2. Matters about which information may be required: search engine

---

21. The incidence of illegal search content and search content that is harmful to children on a service.
22. The number of users who are assumed to have encountered illegal search content or search content that is harmful to children.
23. The formulation, development, scope and application of the statements of policies and procedures mentioned in sections 27(5) and 29(5).
24. The systems and processes for users to report search content which they consider to be illegal content or content that is harmful to children, or other content which they consider breaches any statements of policies and procedures which have been made publicly available by the provider of a service.
25. The systems and processes that a provider operates to deal with illegal search content and search content that is harmful to children, including systems and processes for identifying such

content and minimising the risk of those kinds of content being encountered by means of the service.

26. Functionalities designed to help users manage risks relating to search content that is harmful to children.

27. The design and operation of algorithms which affect the display, promotion, restriction or recommendation of illegal search content or search content that is harmful to children.

28. Measures taken or in use by a provider to comply with any duty set out in Chapter 3 or 4 of Part 3 or section 39 (including in particular measures that are described in a code of practice under section 41).

29. Arrangements that a provider has in place for the reporting (in the United Kingdom or elsewhere) of content relating to child sexual exploitation and abuse, and measures taken or in use by a provider to comply with a requirement under section 66.

30. Measures taken or in use by a provider to comply with any duty set out in section 75 (deceased child users).

31. The systems and processes by which a provider assesses the risk of harm to individuals from illegal search content or search content that is harmful to children—

- a) when the service is initially being designed or developed,
- b) when any further development or update to the service is being considered, and
- c) while the service is in operation.

32. The systems and processes that a provider operates—

- a) to direct users of the service to information about how they can protect themselves from harm in relation to illegal content and content that is harmful to children, and
- b) to counteract or provide support to users of the service in relation to illegal search content and search content that is harmful to children.

33. Co-operation by a provider with government, regulatory or other public sector bodies in the United Kingdom, in particular those involved in the enforcement of the criminal law.

34. Measures taken or in use by a provider to provide a higher standard of protection for children than for adults.

35. Measures taken or in use by a provider to improve the media literacy of users, and an evaluation of the effectiveness of such measures.

36. Any other measures taken or in use by a provider which relate to online safety matters.