Consulting on our Impact assessment of Ofcom's approach to transparency notices

Consultation

Published: 26 November 2026
Closing date for responses: 20 January 2027

Welsh version available

For more information on this publication, please visit ofcom.org.uk.

Contents

Section

1. Overview 3
2. Introduction 5
3. Our approach to transparency reporting 10
4. Reporting period and submission 18
5. Impact Assessment for our approach to transparency reporting 19
6. Consultation Question 25

Annex

A1. Matters about which information may be required 26
A2. Equality and Human Rights impact assessments and Welsh language assessment 29
A3. Information requirements for Category 1 and 2B services 33
A4. Information requirements for category 2A services 34
A5. Illustrative cost assessment of the impact in year 1 35
A6. Evidence 40
A7. Responding to this consultation 42
A8. Ofcom's consultation principles 44

1. Overview

1.1 We are seeking views on our impact assessment of Ofcom's general approach to determine the information requirements for each set of annual transparency reports as part of our duty to issue transparency notices to categorised services (which we refer to in this document as our "approach to transparency reports"). Our impact assessment has considered the costs and benefits of our approach to transparency reports.

1.2 This consultation is limited to our impact assessment as we consulted previously on our overall approach to transparency reporting as part of our consultation on our Transparency Reporting Guidance.

What are we consulting on?

We are consulting on our assessment of the likely impact of implementing our approach to transparency reports.

What have we impact assessed?

We have impact assessed our approach to transparency reports, which is how we will fulfil the two primary objectives set out in our Transparency Reporting Guidance: to deliver an effective transparency reporting regime that will drive improvements on services, and to empower UK users with information to live safer lives online.

What is our approach to transparency reporting?

Core and thematic topics

In our guidance, we established that we would consider a set of '**core'** information requirements to be reported by providers in consecutive notices. We have decided that these core information requirements should focus on the safety systems and processes on services to manage the risks of harms under the Online Safety Act 2023. This document explains our rationale for the topics selected:

- Taxonomy;
- Child user protections;
- Content moderation;
- Reporting and complaints;
- Content recommender systems;
- Misinformation and disinformation;
- Media literacy;
- Deceased child users.

Our guidance also states that we may seek information on a '**thematic'** topic that we ask about on an ad-hoc basis, reflecting Ofcom's regulatory focus in a given year. We have decided that the first set of transparency notices will require relevant services to publish information on grooming, given the potential for transparency in this area to drive safety improvements.

How we tailor information requests to services

We also set out in this document how we will take into in account the six factors set out in paragraph 37 of Schedule 8 to the Act.

Next steps

1.1 This consultation runs from 26 November 2026 to 20 January 2027, and responses should be submitted by 20 January 2027 to OS-Transparency@ofcom.org.uk.

1.2 During the consultation period, we plan to hold a stakeholder webinar. This consultation will run concurrently with our separate process to seek representations from categorised service providers on the draft transparency notices for the services they provide. We will consider all consultation responses and representations received before publishing our statement and issuing final transparency notices.

2. Introduction

Background

2.1 The Online Safety Act 2023 (the "Act") introduced a transparency reporting regime for categorised services. Under this regime, Ofcom has powers to require providers of categorised services to publish certain information about their services in public transparency reports. Ofcom intends for the information published through the regime to deliver an effective transparency reporting regime that will drive improvements on services, and to empower UK users with information to live safer lives online.

2.2 These aims are consistent with the Act which states that the duties imposed on providers seek to secure, among other things, that services regulated by the Act are safe by design; and designed and operated in such a way that: a higher standard of protection is provided for children than for adults, users' rights to freedom of expression and privacy are protected, and transparency and accountability are provided in relation to those services.

2.3 In July 2025, Ofcom published its statement on Online Safety Transparency Reporting.[1] The statement set out Ofcom's guidance on the operation of the transparency reporting regime (the "Transparency Reporting Guidance"). It explained the process for issuing transparency notices, how Ofcom will engage with regulated services and other stakeholders throughout the reporting cycle, and how information from providers' transparency reports will be used to produce Ofcom's own transparency reports.

2.4 The Transparency Reporting Guidance also set out our approach to deciding what information providers would be required to include in their transparency reports. The approach is intended to support an effective transparency reporting regime that drives improvements on services and empowers UK users with information to live safer lives online and ensure that the information we require providers to report is relevant, appropriate and proportionate, and tailored to reflect how individual services are designed, used and operated.

2.5 The Transparency Reporting Guidance set out that some information could be required consistently over time as core information requirements, while thematic information requirements could focus on priority areas. It explained that we would consider opportunities to require the same information across multiple services, where this would enable meaningful comparisons.

2.6 Since publishing that Transparency Reporting Guidance, Ofcom has developed how it will implement its approach to transparency reports. This includes identifying core and thematic information requirements, considering how those requirements should be allocated across different services, and assessing the extent to which they would support the objectives of the transparency reporting regime.

[1] Ofcom, 2025, Statement: Online Safety Transparency Reporting.

Legal Background

Ofcom's general duties under the Communications Act 2003

2.7 Ofcom is the independent regulator for communications services in the UK. We have regulatory responsibilities for the telecommunications, post and broadcasting sectors, as well as for online services. As a public authority, we must act lawfully, rationally and fairly.

2.8 The Communications Act 2003 (the "2003 Act") places duties on us that we must fulfil when exercising our regulatory functions. Our principal duty in carrying out our functions is:

- to further the interests of citizens in relation to communication matters; and
- to further the interests of consumers in relevant markets, where appropriate by promoting competition.[2]

2.9 In performing that principal duty, we must have regard to principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases where action is needed, and any other principles appearing to Ofcom to represent the best regulatory practice. Furthermore, in carrying out our functions, Ofcom is required, among other things, to secure the adequate protection of citizens from harm presented by content on regulated services, through the appropriate use by such services of systems and processes designed to reduce the risk of such harm.

2.10 Ofcom must have regard to the following, among other things, when carrying out its principal duty:

- the vulnerability of children and of others whose circumstances appear to Ofcom to put them in need of special protection; and
- the opinions of consumers in relevant markets and of members of the public generally.

2.11 The 2003 Act requires[3] that Ofcom must have regard to several factors, as they appear to us to be relevant in the circumstances, and as a result we have carefully considered the following in relation to developing our proposals:

- the risk of harm to citizens presented by regulated services;
- the need for it to be clear to providers of regulated services how they may comply with their duties set out in Chapter 2, 3, 4 or 5 of Part 3, Chapter 1, 3 or 4 of Part 4, or Part 5 of the Online Safety Act 2023;
- the need for a higher level of protection for children than for adults;
- the need to exercise our functions so as to secure that providers of regulated services may comply with such duties by taking measures, or using measures, systems or processes, which are (where relevant) proportionate to—

i) the size or capacity of the provider in question, and
ii) the level of risk of harm presented by the service in question, and the severity of the potential harm;

[2] Section 3(1) of the 2003 Act.
[3] Section 3(4A) of the 2003 Act.

- the desirability of promoting the use by providers of regulated services of technologies which are designed to reduce the risk of harm to citizens presented by content on regulated services; and
- the extent to which providers of regulated services demonstrate, in a way that is transparent and accountable, that they are complying with their duties set out in Chapter 2, 3, 4 or 5 of Part 3, Chapter 1, 3 or 4 of Part 4, or Part 5 of the Online Safety Act 2023.

Ofcom's duties in relation to transparency notices

2.12 Section 77 of the Act requires Ofcom to issue an annual transparency notice to each provider of a categorised service. The transparency notice must specify the information to be produced in the transparency report, the format of the transparency report, as well as the date on which the report must be submitted to Ofcom and the manner and date by which the report must be published.

2.13 Ofcom also has a duty under section 159 of the Act to publish their own transparency reports. Information obtained through transparency notices supports Ofcom in performing that function by enabling us to publish aggregate analysis and insights regarding online safety risks and the measures providers take to address them.

2.14 In determining the information to be included in a transparency report, Ofcom may only require information about the matters specified in Parts 1 and 2 of Schedule 8 to the Act (as applicable) and must take into account the factors set out in paragraph 37 of Schedule 8 when determining what information to include in respect of a particular service, which factors include:

- the kind of service it is;
- the functionalities of the service;
- the number of users of the service;
- the capacity of the provider;
- 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[4];
- the proportion of users of the service who are children.

Why we have conducted an impact assessment

2.15 Under section 7 of the Act[5], Ofcom must carry out and publish an impact assessment in cases where we are proposing to do something for the purposes or in connection with the carrying out of our functions; and where it appears to Ofcom that the proposals are "important". A proposal is important if it involves a major change in Ofcom's activities or, where it is likely to have a significant impact on persons carrying out businesses in the markets in relation to which Ofcom has functions, or on the general public.

[4] The relevant duties are set out in Chapters 2 and 3 of Part 3 and Chapters 1 to 4 of Part 4 of the Act.
[5] As amended by section 93 of the Act.

2.16 As a matter of policy, Ofcom is committed to carrying out impact assessments in the great majority of our policy decisions. Our Impact Assessment Guidance sets out our general approach to how we assess and present the impact of our proposed decisions.[6]

2.17 As set out in section 7(5) of the 2003 Act, Ofcom has discretion as to the substance and form of an impact assessment, and this will depend on the proposals being made. However, impact assessments which relate to proposals for the purposes of the carrying out of Ofcom's online safety functions under the Act must include an assessment of the likely impact of implementing the proposal on small and micro-businesses.[7]

2.18 This consultation presents our impact assessment for our approach to transparency reports as we consider this likely to have a significant impact on businesses and the general public. Our impact assessment assesses our approach to transparency reports that will be used every year. While we include in this consultation an illustrative assessment of the likely direct costs that service providers could incur from complying with the information requirements in the first year (see Annex 5), we are impact assessing our approach to transparency reports generally**,** which may result in notices that have a greater or fewer number of questions in any given year. Should we revise our approach to transparency reports in the future, we will consider whether we should carry out a further impact assessment in relation to such a change.

2.19 Our impact assessment builds on stakeholder feedback and considerations made in previous impact assessments including for our Transparency Reporting Guidance.

Growth duty

2.20 Ofcom is also required, when exercising our regulatory functions, to have regard to the desirability of promoting economic growth, including by ensuring that the regulatory action we take is necessary and proportionate.[8] This duty is referred to as the 'growth duty', which has applied to our online safety functions since April 2026.

2.21 We are required to have regard to the UK Government's statutory guidance on the growth duty.[9] That guidance explains that the duty needs to be considered alongside our other statutory duties, and that its purpose is not to achieve or pursue economic growth at the expense of necessary protections.[10] Among other things, it also identifies particular drivers of economic growth, including innovation, investment and competition.

2.22 We have had regard to the desirability of promoting economic growth in this consultation through our consideration of the wider economic impacts of our proposals, including on the providers of categorised services who must comply with the transparency notices.

[6] See Ofcom, 2023. Impact Assessment Guidance.
[7] Sections 7(4A) and 7(4B) of the 2003 Act, as amended by section 93(4) of the Act.
[8] Section 108 of the Deregulation Act 2015.
[9] Section 110(3) of the Deregulation Act 2015.
[10] Department for Business and Trade, 2024. Growth Duty: Statutory Guidance.

Statement of Strategic Priorities

2.23 Under section 92 of the Act, Ofcom has a duty to have regard to the UK Government's SSP for online safety when exercising our regulatory functions on online safety matters.[11] We have had regard to the Statement when carrying out this impact assessment, including the government's prioritisation of "transparency and accountability of online platforms", and the need to drive increased trust in services and expand the evidence-base to provide safer experiences for users.

What we are consulting on

2.24 We have already consulted on the overall transparency reporting framework as set out in our Transparency Reporting Guidance (see paragraphs 2.4-2.5). This consultation assesses the impact of the approach we propose to use, within that framework, in order to determine:

- the core and thematic information requirements which we will ask categorised services year on year; and
- how these information requirements will be allocated to specific services.

2.25 In assessing the impact of our approach to transparency reports, we have particularly focused on, where possible, the costs, benefits and risks of our approach in relation to the UK public and businesses. We have also considered the 'growth duty' (see above), and the impact of our proposals on human rights, specifically the right to freedom of expression and the right to privacy, as well as the impact on specific groups of persons, including persons sharing protected characteristics identified in equality legislation. Our Human Rights and Equality Impact Assessments are set out in Annex A2.

2.26 In accordance with section 7(4) of the 2003 Act, we have also considered how, in Ofcom's opinion, the proposals secure or further the performance of Ofcom's general duties under section 3 of the 2003 Act. We consider that our approach further those duties by improving transparency regarding online safety risks and the systems and processes regulated services use to address those risks, thereby supporting effective regulation and greater accountability of regulated services.

[11] DSIT, 2025. Final Statement of Strategic Priorities for Online Safety.

3. Our approach to transparency reporting

3.1 We explain in our Transparency Reporting Guidance that the specified information required to be published in transparency reports must be relevant, appropriate and proportionate in the context of our policy objectives, which are in turn underpinned by the statutory framework. Our primary stakeholders are users and advertisers, who we believe are likely to benefit from our objectives to deliver an effective transparency reporting regime that will drive improvements on services, and to empower UK users with information to live safer lives online.

3.2 This section sets out and explains our approach to transparency reporting, including how we will apply it to determine the transparency notices for providers (including the 'core' information requirements we ask year-on-year and the 'thematic' information requirements we ask on an ad-hoc basis), and how we have considered the factors set out in our Transparency Reporting Guidance to ensure that information requirements are proportionate, relevant and appropriate to each service.

Our approach to transparency reporting

3.3 We tailor transparency notices for each categorised service by identifying the core and thematic information requirements relevant to that service taking into account the matters set out in Part 1 and Part 2 of Schedule 8 to the Act (as applicable) and the six factors set out in paragraph 37 of Schedule 8 to the Act.

3.4 Transparency reporting under the Act covers information relating to a wide range of online harms and the measures providers may use to address them. We focus our core information requirements on a set of cross-cutting systems and processes that are particularly important to understand how providers identify, manage and mitigate online safety risks across a broad range of harms. This enables us to obtain meaningful information about how providers address different harms through comparable systems and processes, rather than seeking detailed information about every harm and corresponding measure.

3.5 We consider that this approach reflects how providers manage harms in practice, and is a more systemic basis for transparency reporting to support consistency and comparability across services. We consider will provide meaningful information about how particular harms of interest to users, advertisers and other stakeholders are addressed. As such, the same information can provide meaningful insights to a wide range of stakeholders with different interests and priorities across services sectors and harms, helping to support both of the policy objectives we are pursuing.

3.6 Alongside these core requirements, thematic reporting allows us to examine a particular priority harm or safety issue in greater depth where there is a strong case for greater transparency. For example, transparency can target the low incentives to report on areas that are harder to understand, to focus on high risk of imminent or severe harm for particularly vulnerable groups such as children, and to improve understanding or drive safety improvements. This complements the breadth provided by core information

requirements with more detailed insights into where transparency could have particular value.

3.7 Our approach will ensure that questions to services are relevant and proportionate, by means of a consistent and objective process: services with similar characteristics should be subject to similar requirements, while also accounting for differences in service-specific characteristics and circumstances. Taken together, this approach is intended to concentrate transparency reporting where it can provide the greatest value, while avoiding unnecessary or disproportionate information requirements.

3.8 In developing our general approach, and to address relevant information gaps, we have also considered the information that providers of categorised services already make publicly available, including through existing transparency reporting, and evidence from other transparency regimes.[12] This allowed us to consider things such as what metrics services are capable of collecting, avoiding questions that are already available about their UK service/s, and to understand providers' general approach to transparency reporting.

Applying our policy approach to determine the information requirements

Core information requirements

3.9 The core information requirements that we propose to use in our approach to transparency reporting are:

- Taxonomy: This topic covers how providers define and categorise different types of harmful content, including how these relate to categories of harm and offences under the Act.
- Child user protections: This topic covers the measures providers use to identify child users and protect them from a range of harms, including through age assurance and other measures designed to provide age-appropriate experiences.
- Content moderation: This topic covers the systems and processes providers use to review, assess and take action in relation to illegal content and content that is harmful to children.
- Reporting and complaints: This topic covers the mechanisms available to users to report potentially harmful content, make complaints and, where relevant, appeal decisions.
- Content recommender systems: This topic covers how content recommender systems work and how providers manage associated risks, including those arising from the widespread dissemination of content and the cumulative harm that may result from personalised recommendations.
- Misinformation and disinformation: This topic covers providers' approaches to addressing misinformation and disinformation, including relevant policies and measures.
- Media literacy: This topic covers the tools, resources and interventions providers offer to help users understand and navigate the content and risks they encounter online.

[12] See Annex 6 for further detail on existing transparency reporting and other transparency regimes considered.

- Deceased child users: This topic covers providers' policies and processes for responding to requests for information relating to deceased child users, including how requests and complaints are handled.

3.10 In developing these core information requirements, we took the matters in Part 1 and Part 2 of Schedule 8 to the Act (as applicable) and identified the topics relevant to those matters that would produce insights into safety performance trends over time, drive improvements by providers and empower users to make informed decisions.

3.11 Additionally, we consider that these topics align closely with the providers' existing duties under the Act, supporting regulatory coherence. Duties such as the Illegal Content Safety Duties, Children's Safety Duties, Risk Assessment duties and reporting and complaints duties, all require providers to have in place systems and processes that work to tackle a range of online safety risks. Our core information requirements focus on many of these cross-cutting systems and processes.

3.12 This alignment should help limit the additional burden associated with annual transparency reporting. In meeting their existing duties and regulatory obligations under the Act, we would expect providers to already collect information and monitor performance in relation how relevant systems and processes operate and perform. Where this information can also be used to respond to transparency notices, this should reduce the extent to which providers need to collect or generate new information specifically for transparency reporting.

3.13 This approach is aligned to Ofcom's own function to secure adequate protection of citizens from harm presented by content on regulated services, through providers using appropriate systems and processes designed to reduce the risk of harm[13].

3.14 In accordance with section 7(4) of the 2003 Act, Ofcom has considered how these proposals secure or further the performance of its general duties. We consider that the proposed approach to transparency reporting furthers those duties by increasing the availability of information about online safety risks and providers' systems and processes for addressing them. Greater transparency supports effective regulation, promotes public understanding of how providers address online safety risks, and contributes to a safer online environment, particularly for children and other users who may be vulnerable to harm.

3.15 In response to our transparency guidance consultation, we received feedback on the importance of engaging with non-regulated stakeholders. As a result, we held roundtable discussions with experts to seek feedback on our policy approach and identify the kinds of insights we should aim to produce. This included civil society organisations,[14] subject-matter experts and other interested parties. Their views on how existing voluntary transparency reports are used, what makes information useful in practice and the kind of insights that would best support safer and more informed choices helped shape the information requirements we developed. We also consulted Ofcom experts to collect input

[13] Section 3(2)(g) of the 2003 Act (as amended by section 91 of the Act).

[14] The civil society organisations were: 5Rights Foundation; Antisemitism Policy Trust; Canadian Centre for Child Protection; Christchurch Call Foundation; Glitch; Human Digital @ MC Saatchi World Services; Institute for Strategic Dialogue; Internet Matters; Internet Watch Foundation; Lucy Faithfull Foundation; Marie Collins Foundation; NAPAC (National Association for People Abused in Childhood); NSPCC; Online Safety Act Network; Refuge; SWGfL; Tech Against Terrorism; Thorn; Which?

about which information the varied stakeholders they engage with would consider valuable.

3.16 The topics in our transparency notices are intended to provide information about how providers identify, manage and respond to different categories of illegal harm and content harmful to children. Reporting across harms will provide greater transparency about how providers' approaches vary between harm areas and allow for changes in their systems, processes and safety measures to be identified over time.

3.17 Quantitative information at a harms level will provide greater transparency about the prevalence and potential impact of different harms and providers' responses to them, including the volume of harmful content identified, reports received and actions taken across different harm areas. Regular reporting will support the monitoring of trends within specific harm areas and enable comparisons across harms, services and reporting periods. This will provide a clearer picture of the relative prevalence of different harms across services and help identify patterns in how harms manifest across services and harm areas.

Thematic information requirements

3.18 In our Transparency Reporting Guidance, we stated that we may have a set of 'thematic' information requirements which we ask about on an ad-hoc basis, focused on areas that Ofcom has identified based on its regulatory focus each year. 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. These requests are tailored as appropriate to the individual services and may differ in scope and scale.

3.19 We use four guiding criteria to determine the thematic focus for each reporting cycle. These criteria are intended to support the objectives of the statutory transparency reporting framework and Ofcom's online safety duties. In particular, they are designed to help ensure that transparency reporting focuses on areas where reporting is most likely to improve understanding of online safety risks, support accountability, and contribute to improved safety outcomes for users. These criteria will inform how we prioritise one issue among the range of potential matters under Schedule 8.

3.20 First, the topic should address a risk of harm that is severe and/or widespread, so that transparency reporting focuses on areas of greatest potential impact on users. Second, it should align with Ofcom's regulatory priorities for the relevant reporting period, having regard to Ofcom's statutory duties and priorities under the online safety regime. Third, it should be an area where there is sufficient policy and evidence development to identify meaningful indicators of provider performance and service design, allowing transparency reporting to generate reliable and informative insights. Finally, it should be an area where increased public transparency is particularly likely to improve understanding, accountability, or incentives for providers to improve their safety measures, consistent with the objectives of the transparency framework.

3.21 For the first year of transparency reporting, we have applied these criteria and selected grooming for child sexual exploitation and abuse (CSEA) as our thematic focus. We consider grooming for CSEA to be one of the most serious online harms affecting children and an area of significant public, stakeholder, and regulatory concern.[15] It aligns closely with Ofcom's strategic priorities, and it is an area where we have developed a substantial

[15] See also Ofcom, Register of Risks, Section 2A (Grooming).

evidence base and understanding of the measures service providers can take to mitigate risks.

3.22 The prevalence and severity of grooming for CSEA, and the strong public interest in protecting children from this harm, also means that information in this area is likely to be of particular interest to parents and carers, civil society, the media and other stakeholders. Recent evidence highlights the scale of this harm. In October 2026, the ONS reported a 6% increase in the prevalence of reported crimes of sexual grooming from 2025 to 2026, up from 7,172 to 7,607 offences.[16] We consider this increases the potential for the insights generated through transparency reporting to be disseminated and acted upon. This can support both pathways through which we expect transparency to drive change: holding services to account for their safety measures and incentivising them to make safety improvements and empowering users to make more informed choices about their lives online.

Tailoring information requirements for services

3.23 In tailoring the information requirements for each service, we must take into account the six factors set out in paragraph 37 of Schedule 8 to the Act. This section sets out how we will do this and, therefore, how we will decide the information requirements for each service.

3.24 In Schedule 8 to the Act the information requirements are split between matters about which information may be required in relation to the user-to-user ("U2U") part of services and search engines. When developing the question bank for any given reporting cycle, we will develop information requirements for both kinds of services, with the intention of U2U services only receiving information requirements about user-generated content and related safety measures and search services only receiving information requirements about search content and related safety measures.

3.25 When considering the statutory factors (see paragraph 2.14 above), we apply the principles of proportionality, relevance and appropriateness. The way we tailor notices takes into account how each service is designed, used and operated and, importantly, considers any inherent risks to users and child users. Our method of tailoring aims to produce information requirements that produce meaningful insights into individual services and that allows for comparison between services where appropriate. As noted in our Transparency Reporting Guidance, we will also consider whether the information has already been provided or published by the service provider and how we can best use our powers to reveal patterns or trends derived from provider transparency reports.

3.26 We will tailor information requirements to individual services through a structured, two-stage process designed to allow us to apply a common and objective methodology across all categorised services, while recognising relevant differences between individual services and providers. Together, this ensures that the requirements ultimately included in each transparency notice are relevant, appropriate and proportionate, and that we seek only what is necessary to achieve our policy objectives, while generating meaningful and comparable insights into safety and risk across services. The two stages are described in more detail below.

16 Office for National Statistics, Crime in England and Wales: Appendix tables, year ending June 2026. (Accessed: 6 November 2026)

Initial rules-based assessment

3.27 The first stage of our tailoring process involves a rules-based assessment to apply the factors to the information requirements under the core and thematic headings. For each individual question, we identify criteria based on the factors in paragraph 37 of Schedule 8 to determine which services are assigned that question. Our approach to deciding them is described in 'Tailoring for U2U services' and 'Tailoring for Search services' below.

3.28 We then compare the list of questions and applicable criteria to the factors relevant to each categorised service in order to generate an initial set of questions that may be applicable to each service.

Service-level assessment

3.29 The next stage of our tailoring process involves a service-level assessment. In this stage, we apply the criteria established during the rules-based assessment to individual services, taking account of the relevant factors and considering whether the resulting information requirements are relevant, appropriate and proportionate for the particular service. We assess the questions assigned during the previous stage both individually and as a collective set of questions. This assessment takes account of the particular characteristics of the service and provider, including their kind of service, functionalities, user numbers, proportion of child users, and duties applicable to the provider. It also takes account of the provider's capacity to consider the likely burden of providing the information.

3.30 Practically, this assessment involves consulting our internal supervision teams, harms experts, research and intelligence analysts, and economic analysts, who assess the process considering the factors to assign information requirements that are relevant and appropriate to individual services.

3.31 Our assessment of this includes considering whether our questions are similar to those set out under other transparency regimes.

Considering "capacity of the provider"[17]

3.32 For both U2U and Search services, we have taken into account the capacity of the service provider to produce information required from the questions by assessing:

- contextual information about their business model (e.g. profit/non-profit) as a proxy for capacity; and
- the size of the service provider (based on the number of users from their service's categorisation group).

3.33 Where our capacity assessment indicated that there was evidence that questions may be too onerous for a provider, we reconsidered the allocation by question priority, burden of the question, and our view of the capacity of the provider.

3.34 We consider that the size of the service provider (based on the service's categorisation grouping) is likely to be a suitable proxy for the financial resources of the provider, and the level of technical expertise which is available to the provider, or which it is reasonable to expect would be available to the provider given its size and financial resources. This is because larger service operators, on average, should have greater financial resources / technical expertise to respond to the notices. We have considered other potential proxies

[17] Paragraph 37(d) to Schedule 8 of the Act.

for capacity (such as number of employees, profitability and revenue) but there are a number of drawbacks, including difficulties in making consistent comparisons, and difficulties in terms of setting meaningful thresholds for capacity levels. We have also noted the challenges associated with using alternative measures of provider capacity, such as technical resources, revenue and profitability, when developing our codes of practice. See our Illegal Harms Statement[18] for more details.

Tailoring for U2U services

3.35 As set out in our Transparency Reporting Guidance, we will consider how the characteristics of each service, including its user numbers, kind of service, functionalities, and proportion of child users indicate particular inherent risks. Where we consider that a likely risk is indicated, we will ask for information to be provided relating to safety measures relevant to those risks. Below we set out examples of how we used this approach to assign questions across the draft transparency notices which we are proposing for reporting in year 1[19]:

- **User numbers and functionalities:** Where a service's user numbers and functionalities indicate that content can be disseminated easily, quickly and widely, we generally propose more extensive requirements across the relevant core topic areas. This applies in particular to Category 1 services.
- **Kind of service:** Where Ofcom's risk profiles[20] indicate that a kind of service is a risk factor for harm from multiple kinds of illegal content and multiple kinds of content harmful to children (e.g. social media service), we propose more extensive requirements in relevant areas such as content moderation, reporting and complaints, and child user protections. Where a kind of service is associated with a particular harm, this may also inform whether relevant thematic requirements apply.
- **Functionalities:** We considered whether individual functionalities, or combinations of functionalities, indicate particular risks. For example, we considered combinations of functionalities associated with an increased risk of grooming when determining which services should receive the thematic requirements on grooming. Questions about particular functionalities are only proposed where the service has the relevant functionality.
- **Proportion of child users:** The proportion of child users on a service informs the extent to which we propose requirements about measures designed to protect children. This applies particularly to questions in the child user protection topic, but also to relevant questions in other topics such as content moderation and reporting and complaints. We do not generally propose child-specific requirements where the number of child users on the service is likely to be de minimis, (determined in a number of ways, including by considering research data).

Tailoring for Search services

3.36 For search services, we take the same overall approach to assigning questions that we take for U2U services, as described in paragraph 3.34 above. Below we set out examples of how

[18] See Ofcom, Protecting people from illegal harms online: Our approach to developing Codes measures, paragraphs 1.159 and 1.163-1.165.
[19] These notices are currently in draft and we will consider service provider representations before issuing final notices.
[20] See Ofcom, Risk Assessment Guidance and Risk Profiles, Part 3, Section 1 (Risk Profiles), and Children's Risk Assessment Guidance and Children's Risk Profiles, Part 3, Section 1 (Children's Risk Profiles).

we used this approach to assign questions across the draft transparency notices which we are proposing for reporting in year 1[21]:

- Where a search services' user numbers, in combination with its functionality, indicate an elevated risk of harm to users, we considered this as a basis to assign questions to services. In doing so, we considered the Category 2A criteria, which combine user numbers and search functionality, as an indicator of risk that large numbers of users can access content via search results. This justified a larger volume of questions across search-specific themes.
- We have assigned search-specific questions from our question bank to search services, and where appropriate, adapted questions to make them relevant to search functionality.
- Where a search service has GenAI search functionality, we have additionally assigned questions relating to GenAI search protections.

[21] These notices are currently in draft and we will consider service provider representations before issuing final notices.

4. Reporting period and submission

Receipt of annual transparency notices from Ofcom

4.1 For the first year of transparency reporting, providers will have four months to respond to their final transparency notices. We consider that this timeframe strikes an appropriate balance between ensuring information is published in a timely way and giving providers sufficient time to respond to their transparency notices.

4.2 We recognise that the first reporting cycle may be more demanding for providers. As providers become more familiar with transparency reporting and establish processes for responding to transparency notices, we expect providers to be able to respond to a shorter response period of two months in subsequent reporting years.

Transparency reporting periods

4.3 The standard reporting period will run from 1 April to 31 March each year. Using a consistent reporting period will provide a common basis for reporting across services and support comparison of information between reporting years.

4.4 For the first reporting year, providers will report on the period from 1 April 2026 to 31 March 2027. Where a relevant duty comes into force part way through that period, providers will only be required to report on the period from which that duty was in force. Duties that have not come into force by 31 March 2027 will not be included in Year 1 reporting.

5. Impact Assessment for our approach to transparency reporting

5.1 This section considers the likely benefits and costs of our policy approach to transparency reports, as explained in section 3 'Our approach to transparency reporting'.

Benefits relating to our approach to transparency reports

5.2 We consider that our approach to transparency notices has two main benefits: to inform and empower users; and to drive improvements on services. We discuss these in more detail below. By focusing on cross-cutting safety measures and systems and processes, we consider that our approach can provide a comprehensive picture of how providers try to protect users. Conversely, we consider that transparency reporting that focuses solely on harms or solely on systems and processes would only offer partial or narrow insights about safety practices.

5.3 In order to achieve these two benefits, providers must publish clear and meaningful information about the risks associated with their services and the systems, processes and measures they use to address those risks. We believe that transparency reporting will add value to the wider public online safety debate as the insights we're seeking are relevant to UK audiences.

Inform and empower users

5.4 Our approach of focusing on information about services' cross-cutting safety measures can give users (including parents and carers) access to information about how services address risks from varied kinds of illegal content and content harmful to children, thereby helping users to make safer choices online.

5.5 For example, by raising awareness about how services manage risky features like continuous or infinite scroll, users can decide if they want to limit their time or that of a child on a service; or knowledge about the outcome of appeals can inform the possible escalation avenues on a service, including how long content may remain on a service before enforcement action. Information about the implementation and uptake of parental controls can also help users, particularly parents and carers, understand how they can make their children's online experiences safer and make informed choices about where their child is safe to participate online. Users can also gain a better understanding of children's experiences on a particular service where services are asked to respond to questions about how they group children into age groups, and how this approach is used to tailor protections and user experiences.

5.6 Our theory of change also considers that intermediaries can amplify such findings as well as translate them into digestible insights for a range of users, including children. For example, user groups concerned about harm to children from pornography may translate information about how age assurance methods are used to deliver age-appropriate experiences into practical resources for parents. Civil society groups concerned by the

dissemination of hate content via content recommender systems may amplify information about the protections different services have in place relating to these systems, and explain the implications for risks faced by users.

Drive safety improvements

5.7 We consider that the availability of public information can influence the behaviour of users, advertisers and investors, creating incentives for providers to improve safety on their service. Providers that compete to attract users, creator communities and advertisers will be able to compare risks and safety interventions, enabling Ofcom and other intermediaries to identify poor and best practice, which we believe can drive reputational incentives to improve service safety.

5.8 We have considered the different ways this can have an impact. For example, providers will be required to map out their policies and enforcement approaches to show how they address relevant harms and offences under the Act (taxonomy topic); this can help academic and civil society experts analyse specific harms, and use those insights to develop awareness campaigns and advocate for safety improvements. Similarly, answering questions about grooming and child safety can inform advertisers whether a particular service is adequately addressing Child Sexual Exploitation and Abuse content before advising brands to run campaigns.

5.9 In addition, the tailoring of notices to service's characteristics (e.g. kind of service, functionalities and user numbers) opens public scrutiny about a services' understanding of their risks, creating incentives for the provider to justify their understanding of user risks, and/or improve existing safety measures to address them. For example, questions about how moderation teams are resourced can help advertisers understand how providers are making accurate and timely decisions, and whether their resourcing function can sufficiently and consistently address the different harms relevant to their service. Questions about processes to check potential risk of new features and functionalities can give confidence to advertisers about a services' internal governance oversight.

5.10 As set out in Annex 6, we have also considered existing transparency reporting by categorised services and evidence from other transparency regimes. This has helped us identify areas where important information is not currently available about UK users and would therefore be of value, or is not reported in a sufficiently consistent or comparable way to get a full picture of how categorised services manage safety risks.

5.11 In conclusion, we believe the core and thematic topics can offer unique insights relevant to the safety of UK users and help drive improvements on services.

Costs relating to our approach to transparency reporting

5.12 In this section we describe the direct / indirect costs arising from our approach to transparency reporting and our growth duty.

Direct Costs

5.13 The Act requires Ofcom to issue an annual transparency notice to each provider of a categorised service. As such, we expect service providers to incur some direct costs in complying with the information requirements. These are likely to comprise of both central costs and question specific costs.

- **Central costs** are those that a service provider would likely incur irrespective of the number or type of questions. These costs will reflect activities such as reviewing the initial notices, identifying relevant questions, coordinating with project teams, compiling responses, agreeing sign-off from senior directors and submitting the final responses to Ofcom. There may also be some additional costs in relation to responding to possible clarifications sought by Ofcom about the submitted information.
- **Question specific costs** reflect costs that service providers will likely incur to respond to an individual question and involve activities such as collating or gathering information, validating the accuracy of that information and providing it to a central team. There may also be some additional costs in relation to responding to possible clarifications sought by Ofcom about the submitted information.

5.14 The costs of responding to transparency notices are likely to vary significantly across service providers. This is highlighted by an illustrative assessment of the likely direct costs for service providers in year 1 in Annex 5. This is because the time and resources required will depend on factors such as complexity of the service, existing processes and the information being requested. Costs are likely to be lower for services receiving fewer questions. In contrast, services receiving more questions may incur higher costs, particularly where information must be collated from multiple teams or systems. However, we would expect the benefits and costs to scale proportionately, such that any additional costs arising with a higher number of questions are expected to be accompanied by a corresponding increase in the value / benefits of the information.

5.15 We also expect that the costs could be mitigated to some extent as many service providers are likely to already collect and/or have processes and systems in place to gather the relevant user insights. This is because many service providers are likely to already track user behaviour (including how users engage with content and use their platform) and should have systems / processes that gather information that is likely to be relevant to the transparency notices. This is further supported by the following:

- A large number of service providers already report similar information in their voluntary transparency reports as shown in Annex 6 'Evidence'. Our analysis suggests that service providers that receive a higher number of questions are more likely to already publish a higher amount of similar information in their transparency reports.
- Some service providers already gather and report similar information as part of complying with their illegal content and children's risk assessment and corresponding record keeping duties in the Act.
- Some service providers are already subject to transparency requirements in other jurisdictions such as Australia and across Europe, for which they have internal resources and processes to produce annual reports.[22]

[22] For example, a number of service providers, including Facebook, Instagram, Reddit, Snapchat, TikTok, YouTube, Discord and Twitch, are subject to information requirements for the Child Access Report in Australia. Similarly, a number of service providers, including Facebook, Instagram, Pinterest, Snapchat, TikTok, WhatsApp, X, YouTube, Google Search, Bing and Pornhub, are required to publish annual transparency reports under the EU Digital Services Act (DSA). See BOSE-full-report-CSEA-sexual-extortion-periodic-notices-Feb2026Update_0.pdf and Implementing Regulation laying down templates concerning the transparency reporting obligations of providers of online platforms | Shaping Europe's digital future.

5.16 Costs will likely be higher in the first reporting year as service providers are likely to need to set up new processes. However, these costs will fall over time as providers become more familiar with the transparency notices and are able to draw on established systems, processes, and reporting arrangements when preparing their responses. This is consistent with the Government's assessment, which assumed that ongoing compliance costs would fall by 50% after the first year.[23]

5.17 While our reporting requirements will impose direct costs on service providers, we consider that our current approach in Section 3 is the most appropriate and proportionate given our duty to issue transparency notices to categorised services. This is because our approach ensures that the costs will scale proportionately to the size of the benefits and ensures that any undue costs are minimised by[24]:

- Allocating information requirements based on the functionalities and risks attributed to the service, which ensures that service providers will publish information that delivers benefits;
- Providing flexibility to service providers in terms of what sampling technique / metrics they can use to answer the transparency question;
- Aligning reporting practices (such as definitions) with those used in other Ofcom workstreams;
- Ensuring that the topic areas and the nature of the questions are aligned to transparency regulations across international jurisdictions (e.g. the EU DSA, Australian CSEA Report)[25]; and
- As part of our next steps, we are planning to work with service providers during the representation stage to better understand the information requested and what could be potentially driving the trends (e.g. external factors) in order to avoid any undue work later on.

5.18 As discussed above, we have conducted an illustrative assessment on the likely direct costs for year 1 in annex 5 to provide an indication of the potential costs associated with our approach. For this, we have adopted an approach that overestimates the costs for service providers as this would allow us to better reflect the associated costs within our analysis and provides us with further reassurance that our approach, even where the costs are overestimated, is still proportionate. We plan to use the representation process to better understand the implications for each service provider.

5.19 As part of the process to develop our approach, we have also considered other approaches to the transparency notices such as focusing the questions on a few key harms or focusing on both key harms, and systems and processes. We note that these approaches would still lead service providers to incur some direct costs as they would similarly need to gather and submit information (including information on their processes / systems). We note that our approach could lead to higher costs than focusing on a few key harms as service providers

[23] See paragraph 203 Online Safety act enactment impact assessment.
[24] This is consistent with the four factors set out by the UK Government. See paragraph 202 Online Safety act enactment impact assessment.
[25] For example, the EU DSA Periodic Reporting looks into content moderation decisions by providers while Australia's periodic reporting covers a range of topics on CSEA such as detection, response and prevention. See Implementing Regulation laying down templates concerning the transparency reporting obligations of providers of online platforms | Shaping Europe's digital future and BOSE-full-report-CSEA-sexual-extortion-periodic-notices-Feb2026Update_0.pdf.

would be providing information on a larger range of harms but we also expect that the benefits of doing so would be higher as users / advertisers be able to access more information on a larger range of harms. We also note that the costs of focusing on a combination of key harms, and systems and process, would likely be higher as it would likely lead to more questions being asked to service providers.

Indirect Costs

5.20 We do not expect that our approach would result in significant indirect costs to providers. Service providers could incur some indirect costs due to users or advertisers reducing their engagement where the information disclosed highlights higher levels of risk. Whilst this could reduce revenue for those who are perceived to be higher risk, users and advertisers may increase their usage of services with lower risk as they better understand the service they are using.

5.21 Over the longer term, if there is reduced engagement with certain service providers due to transparency disclosures, it could incentivise them to reduce user risks and improve their measures, thereby leading to wider benefits over time. This could mean that users and advertisers could increase their use of a service, which increases future revenue.

5.22 We have considered other approaches as discussed above and we do not expect these approaches would lead to a significantly different impact to the above. For example, focusing on a few key harms could lead to lower indirect costs (as users / advertisers may change their behaviour less as they have less information) but we also note that the corresponding benefits will be lower.

Growth duty

5.23 In considering our approach to transparency reports, we have had regard to the desirability of promoting economic growth. We expect any adverse impact on UK economic growth from our approach to transparency reports to be limited. The transparency duties will impose costs for service providers (which could affect their ability or incentives to invest and innovate) but this is likely to be mitigated to some extent as discussed above. We also expect there could be positive impacts on competition, innovation and/or investment which could support economic growth – this is because the transparency notices could:

- Support growth of service providers with stronger safety practices as transparency notices could lead users and advertisers to increase their usage of these services;
- Support growth in the online news sector by strengthening user trust in service providers with stronger processes to detect and prevent misinformation and disinformation;
- Enhance competition by enabling users and advertisers to make more informed choices between services, thereby encouraging service providers to compete on improving safety practices;
- Help reduce the likelihood of online safety incidents (e.g. children seeing risky content), which reduces the resulting impact and costs for service providers to handle these incidents; and
- Continue to enhance positive online user experiences on categorised platforms, including for the creative industry, SMEs, educational initiatives, thereby fostering new business models that operate in a safer environment.

Provisional conclusion regarding our impact assessment

5.24 Our provisional conclusion is that our approach to transparency reports is unlikely to impose burdens on service providers that are disproportionate to the corresponding benefits.

5.25 We consider that transparency notices could deliver substantial benefits as it enables users to make safer choices online and ensures that service providers have the incentives to make safety improvements and that our approach to transparency reports is consistent with achieving these benefits.

5.26 We consider that our overall approach to transparency reports is proportionate as the focus on cross-cutting safety measures, and systems and processes will be likely to deliver the greatest benefits as it provides a more complete picture of the sector and enables comparability across a diverse range of services, while preserving insights into how services manage risks under the Act.

5.27 While our approach to transparency reports would impose costs on service providers, we consider that it would ensure that service providers will only need to respond to questions that could deliver benefits and it further ensures that the benefits of the overall notice will rise in line with costs. We also expect that the costs to service providers could be mitigated to some extent as many service providers should already have the processes and systems in place to gather and respond to the questions. For example, a large number of service providers already report similar information in their voluntary transparency reports.

6. Consultation Question

6.1 “Do you agree with the impact assessment of our approach to transparency reporting”?

A1. Matters about which information may be required

A1.1 This Annex contains the list of matters in Schedule 8 to the Act about which kinds of information may be required about online safety matters from Category 1 and 2B user-to user services (Part 1) and Category 2A search services (Part 2).[26] There are special rules that apply to which of these kinds of information may be required of a combined service, depending on the parts of Ofcom's register of categorised services it is listed under.[27]

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).

[26] Parts 1 and 2 of Schedule 8 to the Act.

[27] Section 77(8) and (9) of the Act. If a combined service 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. If a combined service is only a Category 2A service and not also a Category 1 or 2B service, then Ofcom may only require the production of search engine information.

11. Measures taken or in use by a provider to comply with the duty set out in section 64(1) (user identity verification).
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.

A2. Equality and Human Rights impact assessments and Welsh language assessment

Equality impact assessment

A2.1 Section 149 of the Equality Act 2010 ('the 2010 Act') imposes a duty on Ofcom, when carrying out its functions, to have due regard to the need to eliminate discrimination, harassment, victimisation and other prohibited conduct related to the following protected characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex and sexual orientation. The 2010 Act also requires Ofcom to have due regard to the need to advance equality of opportunity and foster good relations between persons who share specified protected characteristics and persons who do not.

A2.2 Section 75 of the Northern Ireland Act 1998 ('the 1998 Act') also imposes a duty on Ofcom, when carrying out its functions relating to Northern Ireland, to have due regard to the need to promote equality of opportunity and have regard to the desirability of promoting good relations across a range of categories outlined in the 1998 Act. Ofcom's Revised Northern Ireland Equality Scheme explains how we comply with our statutory duties under the 1998 Act.[28]

A2.3 To help us comply with our duties under the 2010 Act and the 1998 Act, we assess the impact of our proposals on persons sharing protected characteristics and in particular whether they may discriminate against such persons or impact on equality of opportunity or good relations.

A2.4 When thinking about equality we consider the potential impacts more broadly and not just in relation to those groups of persons that share protected characteristics identified in equalities legislation (see paragraph 4.7 of our Impact Assessment Guidance).[29]

- In particular, section 3(4) of the Communications Act 2003 also requires us to have regard to the needs and interests of specific groups of persons when performing our duties, as appear to us to be relevant in the circumstances. These include:
  - i) the vulnerability of children and of others whose circumstances appear to us to put them in need of special protection;
  - ii) the needs of persons with disabilities, older persons and persons on low incomes; and
  - iii) the different interests of persons in the different parts of the UK, of the different ethnic communities within the UK and of persons living in rural and in urban areas.

A2.5 We examine the potential impact our policy is likely to have on people, depending on their personal circumstances. This also assists us in making sure that we are meeting our principal duty of furthering the interests of citizens and consumers.

[28] Ofcom, 2025. Revised Northern Ireland Equality Scheme for Ofcom.
[29] Ofcom, 2023. Impact assessment guidance.

A2.6 We have therefore given careful consideration as to whether the proposals in this consultation will have a particular impact on persons possessing protected characteristics (including race, age, disability, sex, sexual orientation, gender reassignment, pregnancy and maternity, marriage and civil partnership and religion or belief in the UK and also dependents and political opinion in Northern Ireland), and in particular the need to eliminate unlawful discrimination, harassment and victimisation against such persons, advance equality of opportunity and foster good relations.

A2.7 We considered issues raised during consultation on the transparency reporting framework in July 2025. Respondents did not identify material concerns relating to impacts on persons who share protected characteristics under the Equality Act 2010. Some respondents highlighted the importance of understanding how automated systems operate and are used by services, while others emphasised the importance of transparency in relation to online safety and the experiences of children and young people. We have considered these points in developing our approach to transparency reports.

A2.8 Overall, we consider that the approach to transparency reports, will secure benefits for persons and groups with protected characteristics. The approach will produce information requirements annually, which target key online safety matters and aim to produce information about how safety measures are implemented to mitigate harms that specifically impact certain groups.

A2.9 Our approach to transparency reporting will make child user protections a core information requirement and grooming a thematic information requirement. The importance of transparency in relation to child safety and the protection of young people online is an issue, which we have considered to be relevant and appropriate to require annual information about, while also considering it appropriate to perform a deep dive into grooming through our thematic information requirements this year. We note that younger users are potentially more vulnerable to harms online and we note these issues are consistent with Ofcom's statutory duties to have regard to the vulnerability of children and others who may require additional protection.

A2.10 Additionally, our approach to transparency reporting will produce information requirements about service providers' media literacy initiatives. This information will benefit particular groups and persons that are specifically targeted online disproportionately, such as women and girls. The information will develop awareness on how providers are takings steps clarify and promote methods users can take to protect themselves from harm and become more aware of the risks that may target specific groups and persons online.

A2.11 We have not identified evidence that our approach to transparency reporting is likely to have a materially greater adverse impact on persons with protected characteristics than on others. We therefore provisionally conclude that significant adverse equality impacts are unlikely.

Human Rights

A2.12 It is unlawful for Ofcom to act in a way that is incompatible with the European Convention on Human Rights (ECHR).[30] Of particular relevance to Ofcom's functions under the Act are the right to freedom of expression (Article 10 of the ECHR) and the right to privacy (Article 8 of the ECHR). In formulating our approach to transparency reporting, we have analysed how these rights could be impacted by our approach. In particular, we have considered the extent to which our approach may affect users' freedom of expression, the privacy and confidentiality interests of service providers, and the privacy and data protection rights of users.

A2.13 Our approach requires providers to report specified information about measures that may affect how users exercise their rights to freedom of expression and association, including measures relating to content moderation, protections for child users and content recommender systems. By making information about these measures publicly available, transparency reporting should help users better understand how services operate and how providers' systems and processes may affect their ability to express themselves, access and interact with content, and associate with others online. It should also provide users and the wider public with greater insight into how providers seek to balance the protection of users from harm with the protection of freedom of expression and association.

A2.14 We have also considered providers' interests in maintaining the confidentiality of information about their services. We recognise that some information required for transparency reporting may be confidential, and have balanced these interests against the benefits of publication. As part of the draft notice process, providers will have an opportunity to identify confidentiality concerns and make representations to Ofcom, which Ofcom will consider before finalising the information requirements. Where publication is justified, we consider that greater transparency can support improvements in industry standards and online safety, while helping users make informed choices about the services they use.

A2.15 We have also considered the impact of our approach on privacy and data protection. In particular, we have considered whether it would be appropriate to require the publication of personal data as part of the information requirements. We have concluded that requiring the publication of personal data would not be appropriate, given the potential impact on providers and users and the associated data protection considerations. Our approach therefore does not require personal data to be published as part of these information requirements.

Welsh language

A2.16 The Welsh language has official status in Wales. To give effect to this, certain public bodies, including Ofcom, are required to comply with Welsh language standards.[31] Accordingly, we have considered:

- the potential impact of our approach to transparency reporting on opportunities for persons to use the Welsh language;

[30] Section 6 of the Human Rights Act 1998.

[31] The Welsh language standards with which Ofcom is required to comply are available on our website. Source: Welsh Language Commissioner, 2016. Compliance Notice – Section 44 Welsh Language (Wales) Measure 2011.

- the potential impact of our approach to transparency reporting on treating the Welsh language no less favourably than the English language; and
- how our proposals could be formulated so as to have, or increase, a positive impact, or not to have adverse effects or to decrease any adverse effects.

A2.17 Ofcom's powers and duties in relation to online safety regulation are set out in the Act and must be exercised in accordance with our general duties under section 3 of the 2003 Act. In formulating our proposals in this consultation, where relevant and to the extent we have discretion to do so in the exercise of our functions, we have considered the potential impacts on opportunities to use the Welsh language and treating the Welsh language no less favourably than English.

A2.18 We considered consultation feedback received in relation to transparency reporting. No specific issues were raised regarding the Welsh language, opportunities to use Welsh, or the accessibility of transparency reporting arrangements for Welsh-speaking users. Providers may want to translate their reporting in Welsh to make the information accessible to relevant Welsh-language audiences.

A2.19 Given the nature of the proposals, which concern information requirements placed on regulated service providers, we do not consider the proposals are likely to have a significant impact on the Welsh language.

A3. Information requirements for Category 1 and 2B services

A3.1 Information requirements for Category 1 and 2B services, and the definitions used, are set out in full in Annex 3 Information requirements for Category 1 and 2B services.

A4. Information requirements for Category 2A services

A4.1 Information requirements for Category 2A services, and the definitions used, are set out in full in Annex 4 Information requirements for Category 2A services.

A5. Illustrative cost assessment of the impact in year 1

A5.1 We have conducted an illustrative assessment of the likely direct costs that service providers could incur from complying with the information requirements in the first year based on the approach to transparency reporting discussed in Section 3. While our impact assessment relates to our overall approach to transparency reporting, we have used this illustrative assessment to quantify the likely scale of costs of our approach to inform that assessment.

A5.2 This section sets out the:

- Potential approach to estimating direct costs; and
- Results on the likely costs

Approach to estimating direct costs

A5.3 We explored a range of possible approaches to estimate costs, and we consider that an approach that identifies a representative question (i.e. a question that represents the burden of the majority of the questions within the notices) would be most appropriate as this could provide an approximate indication on the scale of costs.

A5.4 We used internal expertise to develop assumptions about the time taken to respond to a representative question and the likely staff that are required (see Table A5.1 below). For total question-specific costs, we multiplied the expected number of questions (including sub-questions) by the cost of responding to a representative question. We estimated the costs for service providers by combining the central costs and sum of the question-specific costs.

Table A5.1: Time taken to complete a notice for service providers

Activities	Time taken in days[32]
Central team – reviewing the notices, establishing governance, senior leader sign-off and submission of the response	5 - 10
Project team – mapping requirements, planning data collection, data processing, internal review and responding to queries	10 - 15

A5.5 Costs to respond to the notices will depend on a range of factors that vary across service providers and some are difficult to incorporate within the analysis. For example, the costs will depend on the internal set up of the service providers, what data is already collected and in what format their information is collected. To account for this, we consider it appropriate to adopt an approach that overestimates the costs. This would allow us to

[32] We have only made assumptions about the number and range of time required for each question, rather than the number of FTEs. This should account for differences in the number of employees involved and also allows for different employees to work on different aspects of the notices simultaneously.

better reflect the associated costs in our analysis and provides us with further reassurance that the notices are proportionate. We have done this by:

- Treating each sub-question (regardless of the size and nature) as its own full question;
- Estimating the costs of all questions whereas some questions may only need to be answered by service providers if that definition applies to them;
- Treating simple yes / no questions and taxonomy questions as the same as more involved qualitative and quantitative questions; and
- Not accounting for the fact that some service providers already gather and report this information.

A5.6 This approach would lead to the costs of some questions to be overestimated and some underestimated, which could lead to this issue being netted out to some extent.[33]

Other cost assumptions

Price level

A5.7 We have used the Annual Survey of Hours and Earnings ('ASHE')[34] to develop estimates for the labour cost required to comply with the information requirements. All quantified estimates of costs or benefits are provided in 2026 prices, unless otherwise stated.

Labour costs

A5.8 Where appropriate, our general approach to estimating labour costs largely uses the same assumptions we used in the April 2025 Statement on Protecting Children from Harms Online ('April 2025 Statement') and in the Additional Safety Measures Statement ('November 2026 Statement).[35] We have done this to ensure methodological consistency across our publications.

A5.9 To develop our estimates for labour costs, we have used the gross median earnings for the occupations corresponding to the Standard Occupational Classification ('SOC')[36] codes listed below. These occupations have been selected on the basis that they best correspond to the job and skill categories we consider would likely be involved in complying with the information requirements.

- **Other professional Occupations (SOC 2)** to cover a range of professions that are employed at various online services and might be required to implement

[33] We note that the DSA included estimates of 0.1 to 2 FTE plus one-off development data collection costs in its impact assessment of its transparency reporting requirements but assumed these were absorbed in the development of systems. We have adopted an approach that considers the costs to collect the data and an approach that overestimates the likely costs as this could provide further support that our approach is likely to be proportionate in year 1. See impact assessment part 1 page 54 Impact assessment of the Digital Services Act | Shaping Europe's digital future.

[34] Office for National Statistics ('ONS'), 2026. Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14 - Office for National Statistics. Data is provisional at time of writing. We previously used earlier versions of the same data set to estimate labour costs, including 2023 ASHE data in the April 2025 Statement on Protecting Children from Harms and subsequently used 2026 ASHE data in the Additional Safety Measures Statement.

[35] https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/online-safety-additional-safety-measures.

[36] We are using Standard Occupational Classification 2020 (SOC 2020), which according to the ONS is the latest update - SOC 2020 - Office for National Statistics.

code measures. This could be legal employees, operations, product managers and so forth.

- **Database administrators and web content technicians (SOC 3133)**[37] to estimate the cost of 'data processing'.

A5.10 For each occupation we are using a salary range to reflect uncertainties surrounding the wages faced by categorised services in the different markets they operate as well as in different seniority levels for the resource required.

A5.11 As a UK-based regulator, we consider it appropriate to use UK earnings for our labour cost estimates. We acknowledge however that in-scope service providers are global enterprises and that in practice, median UK wage rates may differ from the wage rates they encounter in different markets. Our salary range intended to reflect the uncertainty around the labour costs faced by in-scope services.

- The lower bound of that range corresponds to median gross full-time earnings for the corresponding SOC code in the ASHE 2026 data (which we have adjusted further by applying a 22% uplift to account for additional costs such as non-wage labour costs, e.g. employers' National Insurance contributions). [38]
- The upper bound, corresponds to double the median gross full-time earnings, to account for the fact that median UK wage rates may differ from the actual salaries paid by some service providers. This may particularly be the case for larger service providers based in the US, where salary levels may be higher, and for categorised services as they are likely to offer highly competitive salaries. In addition, the salaries may also be considerably higher for some specialist roles. Our salary range is sufficiently wide in order to account for this, but we acknowledge that it may under-represent the labour costs faced by some in scope services.

A5.12 Conversely, service providers may outsource some relevant work to locations where average pay is lower than the UK, which may reduce costs. To the extent this is the case, our salary range may overstate costs.

A5.13 Table A5.2 summarises the labour costs for each of the listed occupations.

Table A5.2: Low and High estimates of Labour costs

Occupation	Low	High
	Annual labour cost estimate	
Other professional occupations	£57,386	£114,772
Data processing	£47,077	£94,155
	Daily labour cost estimate	

[37] This four-digit SOC 2020 code (unit group code 3133) includes occupations such as content, chat, web, and website moderators as well as other occupations such as database administrators and web content. technicians.

[38] ONS recommends dividing the 'employer's social contributions (D.12)' by 'wages and salaries (D.11)' to arrive at the uplift. Both series are published as part of the annual UK National Accounts: Blue Book time series. They provide economy wide estimates of D.11 and D.12 annually. At time of writing, the most recent data available is for 2024.

Other professional occupations	£252	£504
Data processing	£207	£413

Source: ONS (2026), Annual survey of hours and Earnings. This includes a 22% uplift. Calculations are performed based on the median gross salary and then uplifted by 22%.

Notes: The figures are based on annual earnings, and we have calculated daily estimates.[39]

A5.14 Where our cost estimates account for input from senior management, we have used salary estimates from other sources. In previous publications, we estimated annual labour cost for senior leaders at £183,000.[40] These estimates have been updated using recent growth in whole economy earnings. The revised annual labour cost range is £212,000.[41]

A5.15 When estimating the labour costs for complying with the information requirements, we multiply our wage assumptions with assumptions about how long we expect providers would need to complete each relevant task.

A5.16 We therefore obtain a range of estimates for labour costs where the lower bound combines the 'low' wage for each relevant occupation (as summarised in Table A5.2 above) with the lower bound of the estimated number of days required to complete a task. The upper bound combines the 'high' wage for each relevant occupation (as summarised in Table A5.1 above) with the upper bound of the estimated number of days required to complete a task.

Costs for transparency notices.

A5.17 Our estimates for the likely costs are shown in Table A5.3 below. [42]

Table A5.3: Indicative costs for service providers across each category

Category	Costs
Cat 1	£390k - £1.2M
Cat 2A	£220k - £660K
Cat 2B	£50k - £1M[43]

[39] The annual wages are derived from the ONS, 2026 Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14 - Office for National Statistics, Table 14.7a Gross annual pay for all employee jobs, 2026 provisional estimates. The daily wages are derived from dividing the annual wages by the number of working days in a year. We assume on average there are 228 working days in a year. This assumes people work 5 days a week and that there are 8 bank holidays and on average people take an additional 25 days leave a year.

[40] This is based on simple assumptions we have made of £150,000 salary for a senior leader, which are then uplifted by the 22% uplift for non-wage labour costs. See Protecting people from illegal harms online, Annex 5: Assumptions on costs and further analysis on costs and benefits.

[41] Using ONS, 2026. AWE: Whole Economy Year on Year Three Month Average Growth (%): Seasonally Adjusted Total Pay Excluding Arrears. we have updated these figures to account for cumulative growth since 2023.

[42] We note that the UK Government has estimated the costs of the transparency requirements under the Act to be roughly £45,000 per year for each service provider (this was based on estimates from Germany's NetzDG). We understand that this estimate does not cover our role to ensure that the notices are proportionate. See Online Safety act enactment impact assessment, see paragraph 203.

[43] Cat 2B services include a large range of service providers, with differing numbers of questions.

A5.18 As discussed above, we have taken an approach that overestimates the likely costs, and we note there are a number of factors that could indicate the costs are likely to be lower:

- We have designed the questions to reduce the burden on service providers. For example, for some quantitative questions in the content moderation section, we have allowed service providers to calculate metrics using their own sampling approach or proxy indicators, which would reduce the burden on services of estimating the relevant metrics.
- We understand that most service providers already collect and publish some of the information we are asking in the transparency notices (see Annex 6) and this overlap is higher for Category 1 providers who are also receiving the most questions. This could therefore indicate that the costs will likely be lower as these service providers will already have processes and systems in place to respond to the notices.
- Similarly, some of the service providers would also have systems / processes in place to respond to transparency notices in other jurisdictions and may therefore incur lower costs as they would only need to provide the information on the UK and/or adapt their processes to do so.
- Furthermore, some requirements under the Act would mean that stakeholders should already have processes in place to collect and monitor certain types of information. For example, transparency requirements may overlap with risk assessments which are used to understand and inform their own choices to manage risk on their service. Risk assessments may require them to gather evidence on the effectiveness of mitigation measures, particularly in relation to content moderation, reporting and complaints, and age assurance. There may also be overlap between the taxonomies used for transparency reporting and risk assessments, which further leads to lower costs.

A6. Evidence

A6.1 The Act gives Ofcom powers to require information on a range of matters set out in Schedule 8 to the Act, including information about a service's systems and processes, design, and operations. A key aim of transparency notices and reports is to improve users' understanding of how providers of categorised services assess and mitigate online safety risks.

A6.2 A key operational consideration for the transparency regime is ensuring that information requirements are proportionate, appropriate, and relevant, including in relation to the availability and nature of relevant information held by services. Our analysis of existing disclosures indicates that many service providers already collect and publish some information that overlaps with the information we expect to ask for in transparency notices, with this overlap being higher for Category 1 service providers. This includes information disclosed voluntarily, to other regulators, or through litigation and enforcement processes. It is important for Ofcom to understand the nature and extent of these disclosures to help inform our approach to determining information requirements in a way that is clear, targeted, and aware of existing practices. At the same time, the existence of disclosures elsewhere does not limit Ofcom's ability to request UK-specific, time-bounded information where appropriate.

A6.3 To support our role in transparency reporting, we undertook research and analysis to help us identify the information requirements that would likely require new information from services, as opposed to information they already disclose. This considered voluntary service transparency reports and information provided to other regulators, as well as what information categorised services already disclose through litigation in relation to a selection of high-priority transparency topics.

A6.4 The primary purpose of this research and analysis was to support Ofcom in developing well-targeted and evidence-based information requirements, by providing insight into whether, and how, service providers hold, generate, and disclose comparable types of information.

A6.5 Secondly, we looked to identify areas where comparatively limited information appears to have been requested or disclosed by service providers to date, highlighting potential areas where Ofcom could add regulatory value in the future. More information can be found in paragraphs A6.7-A6.12 below.

A6.6 Additionally, in April 2026, we held a series of roundtable discussions on transparency reporting. These sessions brought together stakeholders from non-regulated organisations with relevant subject matter expertise to help inform our approach, such as what information online service providers should publish. Among other things, the discussions explored how stakeholders currently engage with existing transparency reports, what makes them useful in practice, and how they use them to inform their work. We also sought views on the types of insights into online safety risks and service design that would be most beneficial to users, as well as the information that could help them make safer and more informed choices online.

Research and analysis

A6.7 In July and August 2026, Ofcom reviewed the reports published by categorised services that publish transparency reports and found that 8 services do not publish any, or very limited transparency reports.[44] We reviewed voluntarily published reports and those required by the Digital Services Act (DSA) in the EU (29 reports), eSafety in Australia, and Infocomm Media Development Authority (IMDA) in Singapore (5 reports). We compared the questions drafted as of July 2026 for inclusion in transparency notices to categorised services with those questions asked in existing reports. We then recorded whether each Ofcom question had already been answered by a service, and where it had, how closely the existing question matched our own.

A6.8 We conducted this analysis for two reasons. First, to understand how much additional work services would need to undertake to answer our transparency questions, helping inform proportionality requirements. Second, to understand the degree to which our planned questions will contribute to new kinds of information disclosures and public understanding of these services, including how this compared to international jurisdictions.

A6.9 We found that on average services have previously answered around a quarter of questions similar to Ofcom's questions. Category 1 services such as Facebook, Instagram, and Snapchat are most likely to have previously answered similar questions in published reports. The top 5 services who have answered the most questions, answered on average 52% of questions that we plan to include in the Notices, compared to 5% for the bottom 5 services which publish transparency reports. We also found that social media services were more likely to have previously answered questions than messaging or marketplace services (social media: 41%, messaging: 24%, marketplace: 14%).

A6.10 Out of the four categories of reporting we analysed, the DSA reporting was the most likely to include questions similar to the question Ofcom plans to ask services, and the IMDA least likely as it covers fewer services. Services have not previously published UK specific data in 99% of cases and rarely have published information specific to any one country.

A6.11 To complement this review, we also examined information made public through relevant recent and ongoing litigation and court proceedings in the United States involving Category 1 and 2A services. Drawing on specialist analysis provided by an external consultant, this work focused on disclosures relating to recommender systems, child user protections and grooming, and considered the extent to which information disclosed through these proceedings aligned with Ofcom's draft transparency information requirements.

A6.12 Taken together, these different sources provided a more comprehensive understanding of whether providers hold the information we propose to request through transparency notices, the extent to which similar information is already disclosed, and where Ofcom's requirements may generate new insights for users and other stakeholders. The analysis helped inform our transparency notice tailoring process and supported the development of well-targeted and evidence-based information requirements.

[44] Quora, Autotrader, Genius, Mumsnet, Steam, xHamster, Bing, and Facebook Deep Dive.

A7. Responding to this consultation

How to respond

A7.1 Ofcom would like to receive views and comments on the issues raised in this document, by 5pm on 20 January 2027.

A7.2 You can download a response form here. You can return this by email or post to the address provided in the response form.

A7.3 If your response is a large file, or has supporting charts, tables or other data, please email it to OS-Transparency@ofcom.org.uk, as an attachment in Microsoft Word format, together with the cover sheet. This email address is for this consultation only and will not be valid after 20 January 2027.

A7.4 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:

- send us a recording of you signing your response. This should be no longer than 5 minutes. Suitable file formats are DVDs, wmv or QuickTime files; or
- upload a video of you signing your response directly to YouTube (or another hosting site) and send us the link.

A7.5 We will publish a transcript of any audio or video responses we receive (unless your response is confidential)

A7.6 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt of a response submitted to us by email.

A7.7 You do not have to answer all the questions in the consultation if you do not have a view; a short response on just one point is fine. We also welcome joint responses.

A7.8 It would be helpful if your response could include a direct answer to the question asked in the consultation document. The question is listed at section 6. It would also help if you could explain why you hold your views, and what you think the effect of Ofcom's proposals would be.

A7.9 If you want to discuss the issues and questions raised in this consultation, please send an email to OS-Transparency@ofcom.org.uk.

Confidentiality

A7.10 Consultations are more effective if we publish the responses before the consultation period closes. This can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish responses on the Ofcom website at regular intervals during and after the consultation period.

A7.11 If you think your response should be kept confidential, please specify which part(s) this applies to and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.

A7.12 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it. But sometimes we will need to publish all responses, including those that are marked as confidential, in order to meet legal obligations.

A7.13 To fulfil our pre-disclosure duty, we may share a copy of your response with the relevant government department before we publish it on our website.

A7.14 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our Terms of Use.

Next steps

A7.15 Following this consultation period, Ofcom plans to publish a statement with our final impact assessment

A7.16 If you wish, you can register to receive mail updates alerting you to new Ofcom publications.

Ofcom's consultation processes

A7.17 Ofcom aims to make responding to a consultation as easy as possible. For more information, please see our consultation principles in Annex 8.

A7.18 If you have any comments or suggestions on how we manage our consultations, please email us at consult@ofcom.org.uk. We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and residential consumers, who are less likely to give their opinions through a formal consultation.

A7.19 If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact the corporation secretary:

Corporation Secretary
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA
Email: corporationsecretary@ofcom.org.uk

A8. Ofcom's consultation principles

Ofcom has seven principles that it follows for every public written consultation:

Before the consultation

1. Wherever possible, we will hold informal talks with people and organisations before announcing a big consultation, to find out whether we are thinking along the right lines. If we do not have enough time to do this, we will hold an open meeting to explain our proposals, shortly after announcing the consultation.

During the consultation

2. We will be clear about whom we are consulting, why, on what questions and for how long.
3. We will make the consultation document as short and simple as possible, with an overview of no more than two pages. We will try to make it as easy as possible for people to give us a written response.
4. When setting the length of the consultation period, we will consider the nature of our proposals and their potential impact. We will always make clear the closing date for responses.
5. A person within Ofcom will be in charge of making sure we follow our own guidelines and aim to reach the largest possible number of people and organisations who may be interested in the outcome of our decisions. Ofcom's Consultation Champion is the main person to contact if you have views on the way we run our consultations.
6. If we are not able to follow any of these principles, we will explain why.

After the consultation

7. We think it is important that everyone who is interested in an issue can see other people's views, so we usually publish the responses on our website at regular intervals during and after the consultation period. After the consultation we will make our decisions and publish a statement explaining what we are going to do, and why, showing how respondents' views helped to shape these decisions.