

Overview of the UKSIC

The UK Safer Internet Centre (UKSIC), established in 2011, is a leading global partnership helping to make the internet a great and safe place for everyone. We provide support and services to children and young people, adults facing online harms, and professionals working with children.

A bridge between Government, industry, law enforcement and society, we are the engine of the online protection landscape in the UK, dealing with both prevention and response.

Formed of three charities, [Childnet](#), [Internet Watch Foundation](#) and [SWGfL](#), we work together to identify threats and harms online and then create and deliver critical advice, [resources](#), education and interventions that help keep children and young people, and adults, safe. We share our best practices across the UK and globally.

We focus our work around four functions:

- **An awareness centre:**
Where we provide [advice and support](#) to children and young people, parents and carers, schools, and the children's workforce.
- **Three helplines:**
Which [provide support to professionals](#) working with children and young people with online safety issues, and support to all adults facing issues with [harmful content](#) and [non-consensual intimate imagery](#) online.
- **A hotline:**
Which provides an anonymous and safe place to [report](#) and remove online child sexual abuse images and videos wherever they are found in the world.
- **A voice to young people:**
We operate a Youth Advisory Board, and we nurture youth participation, providing a focus on youth voice to give young people agency to make a difference in their school communities.

UKSIC is the proud coordinator of Safer Internet Day in the UK.

Our partners the IWF and the SWGfL have submitted responses to this consultation and we fully endorse their responses. We have summarised and integrated their responses where appropriate. Please refer to their full responses for the detail.

Question	Your response
We welcome input from industry on the areas listed below. We encourage stakeholders to respond with feedback so that we can ensure that the guidance helps providers and other stakeholders understand:	
A) Ofcom's powers and providers' duties for transparency reporting, as well as Ofcom's approach to implementing the transparency regime.	Confidential? – N Transparency reporting and Concerns As UKSIC, we support the transparency process as set out in the Online Safety Act. One of the key aims of this initiative is to underscore that transparency reporting

B) Ofcom's approach for determining what information service providers should produce in their transparency reports.

C) Ofcom's plans to engage with providers prior to issuing transparency notices, and on what matters, and whether the proposed engagement plan will be sufficient for helping services to comply with their duties.

D) Ofcom's plans to use the information in providers' transparency reports in Ofcom's own transparency reports.

serves as a powerful lever for positive change within companies. This outcome-focused view is intended to drive improvements in both service providers' behaviour and actions, as well as in user behaviours and actions. The guidance has been carefully structured to help achieve these goals.

Central to this approach are three key principles: relevance, appropriateness, and proportionality. Relevance ensures that the information requested is meaningful and tailored to the specific service. Appropriateness demands that the data provided is useful, contextual, and aligned with the service's duties. Proportionality ensures that only the information necessary to deliver the policy's objectives is sought.

Ofcom's guidance recognises the importance of tailoring information requirements based on the type of service and its users. It explains the factors that will be considered when deciding what information is required, ensuring that the requests are both reasonable and aligned with the overarching aim of creating safer online environments. This balanced approach will enable transparency reporting to drive positive outcomes without placing undue burdens on service providers.

However, we hold concerns regarding the effectiveness of the transparency process, particularly the reliance on the goodwill and honesty of corporations. These companies, which operate for profit and are shareholder-driven, may not always prioritise transparency and user safety over financial interests. There is a general dissatisfaction with an approach that hinges on voluntary corporate compliance, which could lead to inconsistent and insufficient reporting.

Reflecting on the feedback from Arturo's report; relying solely on voluntary cooperation from corporations may not achieve the desired outcomes, as it risks incomplete or selective reporting.

We acknowledge that ofcom has taken on board Arturo's ideas about the importance of metrics that measure users' experiences of harmful content. Ofcom agrees that understanding the impact of harm on users is crucial for evaluating the effectiveness of

	online safety measures. They already conduct extensive research with UK citizens, including children, about their experiences of risk and harm online. As noted in the guidance, this research can be incorporated into Ofcom’s transparency report where relevant. The enforcement aspect is still yet to be discovered and the checks and balances systems should incorporate civil society groups and other actors who could provide accurate and objective data on the actual experiences of users online including the most vulnerable. While the guidance outlines factors that Ofcom will use to decide what information to require, there is a risk that corporations may offer minimal compliance, adhering to the letter rather than the spirit of the law. This could undermine the objectives of the Online Safety Act, as profitdriven motives may conflict with the desire to foster safer online environments. Therefore, we advocate for more robust oversight and mechanisms to ensure true transparency and accountability. The current provisions assume that companies will adopt a goodwill and transparent self-assessment process which unfortunately is not reflecting reality. Arturo Bejar, the Meta whistleblower who has recently testified to the US Congress, observed: “Social media companies are not going to start addressing the harm they enable for teenagers on their own. They need to be compelled by regulators and policy makers to be transparent about these harms and what they are doing to address them. Helplines and Trusted Flagger As the official UK Intimate Image Abuse helpline (Revenge Porn Helpline) we have first-hand experience with victims of online abuse, who have sought out help through our service. We would therefore like to see the introduction of a Trusted Flagger system, where the helplines operated by SWGfL and other legitimate stakeholders could share information, practices and be in constant communication with Ofcom and online services. This process could also act as an extra online safeguarding step which will reinforce or refute the findings of the service provider self-assessment and child user condition document. We would also like to point Ofcom to the direction of the Guidelines
--	--

	and best practice for the trusted flagger relationship between helplines and online service providers document which was developed by the Early Warning Working Group of the UK Council for Internet Safety, and published in April 2023, see https://www.gov.uk/government/publications/trusted-flagger-programmes. The trusted flagger system can act as a significant step of accountability where it could, act as an extra checks and balance step to ensure that the data and information provided by service providers in the transparency report is accurate and reflecting on the actual experiences of the most vulnerable users online. UKSIC therefore recommends the inclusion of Civil Society Groups to be added to the list of collaborators on P.17. Through the process of engaging stakeholders Ofcom can achieve an inclusive, holistic and objective transparency and information gathering process which will pave the way for further online safety provisions and development. Super Complaints Another significant step to reflect on the accuracy of the data and information in the transparency report is the introduction of a Super-Complaints process. The current provisions as set out in previous consultations, impose significant resource implications to eligible bodies to the point that it could prevent them from putting forward any submissions due to complexity and costs. An organisation could take a significant time to be able to build conclusive evidence and build a file report that matches the description that is provided by this draft. While the proposals in Chapter 16 of the Illegal Harms Consultation establish a framework for reporting and complaints, the integration of ADR mechanisms could significantly improve the effectiveness, accessibility, and user trust in these processes. Leveraging SWGfL's expertise in online safety underscores the pivotal role ADR can play in the broader ecosystem of reducing online harm and resolving disputes. Additionally, we think that Ofcom should streamline the process to ease the entry of organizations who are planning to submit a sufficient and full super-complaint. Accordingly, the Super Complaints entity
--	--

	requirement outlined in S.169 of the Online Safety Act, sets out Ofcom as the sole responsible body to make the inspection and provide the final verdict. That fact leads to the lack of an alternative body for any individual complaints, while also intrinsically delaying the process and outcome leading to aggravated harm to the victims.
Are there any aspects in the draft guidance where it would be helpful for additional detail or clarity to be provided?	Confidential? – N
Are the suggested engagement activities set out in the draft guidance sufficient for providers to understand their duties and Ofcom’s expectations?	Confidential? – N ADR and offering users the right to recourse The lack of a structured approach to alternative dispute resolution (ADR) in the proposals represents a missed opportunity to bolster user trust and platform accountability significantly. ADR offers numerous advantages, such as easing the burden on formal complaints processes, fostering more positive relationships between platforms and users, and potentially resolving conflicts in a manner that respects the interests of all involved parties. Additionally, ADR mechanisms like mediation, arbitration, or ombudsman services can bring expertise and impartiality that may not always be present in platform-driven complaints procedures. SWGfL suggests that the proposals could be enhanced by explicitly integrating ADR mechanisms into platforms' strategies for addressing complaints and disputes. An outline of an ADR solution previously proposed by SWGfL in the illegal harms consultation; this could be supplemented by the development of specific guidance or standards for ADR mechanisms within the context of online harms. This would include criteria for mediators or arbitrators and processes that ensure fairness, transparency, and accessibility. Referencing Report Harmful Content, the Draft Online Safety Bill (Joint Committee), in December 2021¹¹ recommended (paragraph 457) that; “The role of the Online Safety Ombudsman should be created to consider complaints about actions by higher risk service providers where either moderation or failure to address risks leads to significant, demonstrable harm (including to freedom of expression) and recourse to

	other routes of redress have not resulted in a resolution” and that “We suggest that the Department look to Report Harmful Content as a potential model for what such an Ombudsman could look like”. The absence of an Alternative Dispute Resolution for users in the online world will leave thousands of users at increased risk of harm. The introduction of the Online Safety Act without the provision of an ADR mechanism will downgrade the impact of the Bill as users will have nowhere to turn if they are being harmed online. This is further exacerbated by the fact that currently users under the VSP regulation can make independent appeals and in effect the implementation of the Online Safety Act will remove that right. The enactment of the Online Safety Act required Ofcom to undertake a review of whether an ADR was required. This was due to commence in October 2023 but has not yet started leaving thousands of users at increased risk. The recent report by the Public Accounts Committee identified the following: <i>“Years may pass before the Online Safety Act (OSA) makes a noticeable difference to people’s online experience. In a report published today, the Public Accounts Committee (PAC) finds that regulator Ofcom has made a good start in preparing for its new role protecting citizens from online harm – but questions remain over how it will manage public expectations for what the regulatory regime will achieve, with the regulator unable to act on individual complaints and overseas providers in particular posing a significant challenge.”</i> The UK Safer Internet Centre and the Report Harmful Content (RHC) service established in 2019, offers a pioneering model for addressing legal but harmful content through ADR. The service underscores the critical role of such mechanisms in holding platforms accountable and ensuring that users' grievances are addressed equitably. Other industries include provisions for ADR processes and checks and balances such as present in financial services and travel agencies. A similar approach and structure
--	---

	could be adopted in the digital world, where individuals and organisations can pursue redress. While the proposals in the illegal harms process establish a framework for reporting and complaints, the integration of ADR mechanisms could significantly improve the effectiveness, accessibility, and user trust in these processes. Leveraging SWGfL's expertise in online safety underscores the pivotal role ADR can play in the broader ecosystem of reducing online harm and resolving disputes. Please find below, the modelling explanation note containing more information on ADR and our proposal.
--	--

Question	Your response
We are also seeking input that will help us understand if there are other matters that Ofcom should consider in our approach to determining the notices, beyond those that we set out in the guidance. The questions below seek input about any additional factors Ofcom should take into account in various stages of the process, including: to inform the content of transparency notices; in determining the format of providers' transparency reports; and how the capacity of a provider can be best determined and evidenced.	
Are there any other factors that Ofcom might consider in our approach to determining the contents of notices that are not set out in the draft guidance?	Confidential? – N Online Safety Online safety and ensuring the platform is safe to use for children to use, should be the priority outcome of the transparency report. Therefore, the transparency process, as suggested by Ofcom should be made public and accessible for parents, teachers, children and anyone who is interested. At the same time, UKSIC is concerned with the inclusion of a safeguarding process within the structure of the services, as the process of transforming a service into one that is safe-by design requires, an organisational commitment to safeguarding measures that are present in each step of the operation. For instance, as UKSIC we would be interested to see if the transparency records or safety levels which would be benchmarked would be featured in the financial reports of these service providers who are eligible under the act. The transparency reporting process should not be treated as just a sign off once a year habit, but

	rather a step forward to ensure a cross sector commitment on safety which will be streamlined across the organisational structure of the service. With regards to thematic information reporting, we are quite unclear on what would constitute core and thematic information, and we are unclear on what would trigger a thematic transparency report. If it was triggered on the occasion of a service causing significant harm, how would Ofcom be alerted to that, and if that were the case, we would expect the thematic transparency report to be published to the public in due time, to prevent any further harm.
Is there anything that Ofcom should have regard to (other than the factors discussed in the draft guidance) that may be relevant to the production of provider transparency reports? This might include factors that we should consider when deciding how much time to give providers to publish their transparency reports.	Confidential? – N
What are the anticipated dependencies for producing transparency reports including in relation to any internal administrative processes and governance which may affect the timelines for producing reports? What information would be most useful for Ofcom to consider when assessing a provider's "capacity", by which we mean, the financial resources of the provider, and the level of technical expertise which is available to the service provider given its size and financial resources?	Confidential? – N Proportionality Focus Ofcom's approach to proportionality appears predominantly economic, aiming to avoid imposing costs on companies. While the Online Safety Act (OSA) mandates that regulated services adopt a proportionate approach in fulfilling their duties, considering provider size and capacity, it also requires attention to levels of risk and the nature and severity of harm. Proportionality should balance the economic impact on companies with the societal costs and prevalence of harms to users, including impacts on the criminal justice system and support services for victims, particularly for women, girls, and minority groups. Severity of Harm Consideration: The severity of harm involves not only the number of affected individuals but also the intensity of the impact. Despite recognizing

	harms in the risk register, Ofcom's code of practice measures do not explicitly consider these aspects. The current focus is more on the economic burden on tech companies rather than balancing it against the societal costs of harm. Small vs Large Companies: Misjudged Proportionality: The proportionality analysis assumes that smaller companies pose less harm due to their limited reach. However, this assumption overlooks the severe harm that can occur to minoritized groups on targeted small sites. The Act includes 53 references to "proportionate," emphasizing that measures should be proportionate to the risk of harm rather than merely considering company size or capacity. Parliamentary Debate Insights: During the Lords Committee stage debate, the Government Minister assured that the child safety duties would be tailored to the size and capacity of providers. Smaller providers still need to meet child safety duties if their services pose a risk to children. These providers must implement systems and processes reflecting their services' risk level, ensuring they achieve the required child safety outcomes. UKSIC therefore proposes the introduction of measures and metrics which do not only measure the size of the service but include a multitude of factors as mentioned in the illegal harms consultation including, the user journey, functionalities and other design choices that could aggravate the risk of harm. At the same time, as mentioned small services can still cause harm to their users, should not be omitted from the service particularly as the current thresholds for the large service categorisation are quite high with 7 million monthly users.
Are there any matters within Schedule 8, Parts 1 and 2 of Act that may pose risks	

relating to confidentiality or commercial sensitivity as regards service providers, services or service users if published?	
---	--

Question	Your response
Finally, we are also seeking input into any matter that may be helpful for ensuring Ofcom's transparency reports are useful and accessible.	
Beyond the requirements of the Act, are there any forms of insight that it would be useful for Ofcom to include in our own transparency reports? Why would that information be useful and how could you or a third party use it?	Confidential? – Y/N Clarity In general, we are very supportive of the inclusion of transparency reports as an important instrument which will provide the necessary basis which will facilitate the information gathering powers of Ofcom. At the same time, recognising the different functionalities of services we would like to see more clarity with regards to the information collected which can be comparable between services. Certain functionalities and design choices can therefore be benchmarked and compared across different platforms. In turn this could provide more context for the public, but service providers who could compare integral part of their services such as terms and conditions, moderating systems with other services and cover any gaps in their safety provisions. As UKSIC we are proposing that Ofcom whenever possible should request comparable and quantifiable metrics that can be compared across platforms. This process of classification could provide the grounds for a cross sector safety-by-design approach that different services can adopt. The transparency report and any other relevant information should also be useful for the user, providing more information and context regarding any services they are using regularly. Ofcom should publish and inform users in an accessible way about the process and any outcomes that come out of the information gathering power process.
Do you have any comment on the most useful format(s) of services' transparency	Confidential? – Y/N

reports or Ofcom's transparency reports? How can Ofcom ensure that its own transparency reports are accessible? Provide specific evidence, if possible, of which formats are particularly effective for which audiences.	
---	--

Question	Your response
Please provide any other comments you may have.	
General comments	Confidential? – /N

Please complete this form in full and return to OS-Transparency@Ofcom.org.uk