Your response

Volume 2: The causes and impacts of online harm

Ofcom's Register of Risks

Question 1:	
i)	Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?
Response: No response	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 2:	
i)	Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.
Response: No response	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Volume 3: How should services assess the risk of online harms?

Governance and accountability

Question 3:	
i)	Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?
Response: No response	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 4:	
i)	Do you agree with the types of services that we propose the governance and accountability measures should apply to?
Response: Microsoft agrees that the proposed governance and accountability measures (i.e., annual reviews of risk management activities and internal monitoring and assurance functions) should be applied to large and multi-risk services.	
ii)	Please explain your answer.
Response: We agree that robust governance processes and regular review are essential to any effective risk management program, particularly for larger regulated services that may pose a greater risk of online harm due to the amount of its monthly active users. We encourage Ofcom to provide larger regulated services additional flexibility to meet the proposed measures outlined in Section 8 of Volume 3 through centralized risk management functions. In practice, within larger organizations some of the referenced governance functions are operated through centralized practices and teams, rather than at the individual service-level. This approach to regulatory governance promotes operational efficiencies, deeper subject matter expertise and economies of scale. For example, many of Microsoft's services are effectively supported through centralized assurance functions.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 5:

i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?

Response: Should a future independent third-party audit measure be proposed, we strongly encourage Ofcom to harmonize the requirements with those found in Article 37 of the Digital Services Act ("DSA") and, like the DSA, apply it solely to large services that present the highest risks to end users.

We agree with Ofcom's view that alignment between existing online safety regulatory regimes promotes compliance while minimizing the burden on business. Harmonization with the DSA's audit requirements can achieve both goals while also enabling further development of a global and standardized approach, supporting effective and consistent safety information-gathering across jurisdictions. Taking this approach would provide clarity for regulated services and allow them to leverage relevant, pre-existing work.

We note that engaging third-party auditors to conduct a top-down review of a compliance program is an expensive endeavour. There are currently few audit firms engaged in this work, as standard methodologies have not been established. Independent audit is also a time and labour-intensive endeavour for companies. The internal resources required to support audit engagements are those knowledgeable of and responsible for core safety compliance within a service. Months of audit engagement take these resources away from their core support for safety improvements in a service. As such, independent audit obligations, particularly where they may be duplicative of work already completed in support of obligations from other jurisdictions, may detract from the overall safety goals of the UK Online Safety Act ("OSA").

ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 6:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?

Response: Microsoft recommends against the use of specific safety outcomes as a significant determination of renumeration, particularly if they are rate-based outcomes (e.g., the presence of illegal content on the service, the number of content items actioned, the number of times users are exposed to illegal content, etc.). Rate-based safety outcomes could be a result of several factors that are not in a senior manager's control, such as under-reporting of illegal content by end users. The measure of "success" could also vary from service to service, making it difficult for services to accurately determine whether they are in "compliance." Rate-based reward systems may also have the unintended consequence of *discouraging* senior managers from seeking or documenting online harm risks or negative outcomes for fear that their renumeration will be impacted; it could even result in an artificial inflation of safety outcomes. Enabling senior managers to dispute a safety-based impact to remuneration introduces even more practical complexity.

Should this measure be included in future guidance as an indicator of a company or service's safety governance practice, we encourage a behaviour-based approach that considers whether services take into consideration positive online safety behaviours as one factor in a holistic review to determine the renumeration for senior managers.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Service's risk assessment

Question 7:
i) Do you agree with our proposals?
Response: Generally, we support Ofcom's proposals on how regulated services can fulfil their illegal content risk assessment statutory duties. But we would encourage Ofcom to permit regulated services the express flexibility to satisfy their requirements under Sections 9 and 26 of the Online Safety Act ("OSA") with previously created risk assessments.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We welcome the clarity and actionable guidance Ofcom has provided on how the required assessments should be completed and what information should be considered. Ofcom's Risk Profiles, especially, are a commendable advancement that simplifies the task of identifying potential illegal harms into a straight-forward, practical exercise. We also support Ofcom's incorporation of current best practices and risk assessment requirements from other jurisdictions, such as Australia and the European Union ("EU") (Volume 3, Sections 9.25 – 9.34). As global online safety requirements continue to proliferate, multi-jurisdictional services will need to find synergies so that they can meet their varying legal obligations and produce high-quality digital safety and compliance results. Given this, we would encourage Ofcom to permit regulated services the express flexibility to satisfy their requirements under Sections 9 and 26 of the OSA with previously created risk assessments. This could be done by accepting previously completed risk assessments that align to emerging international standards (such as the Digital Trust and Safety Partnership Safe Framework) and other regulatory regimes as "suitable and sufficient", based on a discussion between the service and the regulator as to adequacy. Mutual recognition among regulators and/or formal standardization of this and other regulatory requirements would have several benefits – it would: 1) enable the further development of in-flight efforts to encode best practices in a way that supports global harmonization and interoperability; 2) encourage predictable, consistent information-gathering by services; 3) promote the recognized benefits that result from an open internet with cross-border data flows (see OECD (2016), "Economic and Social Benefits of Internet Openness", *OECD Digital Economy Papers*, No. 257, OECD Publishing, Paris, https://doi.org/10.1787/5jlwqf2r97g5-en); 4) reflect the important role that individual company terms of service play in reducing harm, in addition to country-specific illegal content requirements; and 5) meet one of Ofcom's key policy objectives by reducing undue burden on services, particularly for providers that have already exerted substantial efforts to identify and assess the risks posed by illegal and harmful content on their service.

We acknowledge that variations exist between the requirements of the UK's OSA and online safety regimes in other jurisdictions, particularly how illegal harms are defined and should be documented in any specific assessment. Should Ofcom adopt our general recommendation, it would be helpful to document the circumstances where previously completed risk assessment will be deemed compliant with Sections 9 and 26 of the OSA in the Service Risk Assessment Guidance (Annex 5 of the Consultative materials). This will help provide regulated services actionable guidance on any additional work that must be completed before any previously created risk assessment will be accepted as compliant.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Specifically, we would also appreciate evidence from regulated services on the following:

Question 8:
i) Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?
Response: Microsoft agrees the four-step risk assessment process and Risk Profiles provide a clear, actionable road map for regulated services to meet their statutory obligations, while still allowing sufficient flexibility to meet Ofcom's goal of being risk proportional and enabling a service-by-service dialogue with the regulator.
ii) Please provide the underlying arguments and evidence that support your views.
Response: No response
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
Response: The Risk Profiles are clear and provide actionable guidance that will help regulated services understand and identify potential risks on their service. However, we provide additional comment on the application of the risk factors, as outlined at Question 15 below.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response: The Risk Profiles are clear and provide actionable guidance that will help regulated services understand and identify potential risks on their service. However, we provide additional comment on the application of the risk factors, as outlined at Question 15 below.	
iv)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 11:	
i)	Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Volume 4: What should services do to mitigate the risk of online harms

Our approach to the Illegal content Codes of Practice

Question 12:	
i)	Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?
Response: This comment applies to Ofcom's overarching approach to the Consultation. Ofcom may wish to consider dividing future consultations into shorter, more manageable pieces to yield the highest quality evidence and optimize accessibility to the material, particularly for smaller services. The extraordinary breadth of content in this ~1700-page Consultation, published all at once, may significantly hinder submitters' abilities to adequately address all 50+ questions with constructive, data-driven feedback and with submission of specific evidence as requested by Ofcom. The sizeable challenge to analyze the Consultation and respond to all questions would be exacerbated for smaller regulated services. We acknowledge the many resources Ofcom provided, such as webinars and chapter summaries, to explain the contents of the Consultation. However, relying on such materials may cause a service to miss important issues that merit its input. For example, Ofcom states it may introduce a future Code of Practice recommending that services use proactive content detection technology to identify first-generation illegal harms, such as CSAM, but the statement is made 60 pages after Ofcom summarizes the input it wishes to receive from services. (See Volume 4, Section 14.328). Stakeholders may therefore miss the opportunity to comment during this Consultation on an issue that merits careful consideration and stakeholder feedback.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 13:	
i)	Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?
Response: We agree that the most risk-proportional approach is to apply the most onerous measures to regulated services that pose relatively greater risks to end-users, dependent on the nature of the service and the risks in question. However, we encourage Ofcom to adjust how it has chosen to define "large services" and "multi-risk services" to more accurately reflect the proportional risk regulated services pose in practice (discussed further at Questions 14 and 15 below).	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 14:
i) Do you agree with our definition of large services?
Response: No, Ofcom's current definition of "large service" may be over-inclusive in practice and should be adjusted so that the definition reflects both size *and* safety risks.
ii) Please provide the underlying arguments and evidence that support your views.
Response: The number of monthly active users has been used in several regulatory regimes as one of several determinative factors when assessing whether a service should be considered high risk. Ofcom's current definition of "large service" may be over-inclusive in practice and should be adjusted so that the definition reflects both size *and* safety risks. To achieve the Online Safety Act's ("OSA") goal to create a risk-proportional regime, only the largest and higher-risk services should be captured in the definition. The proposed seven million user threshold has been calculated largely using one factor: the Digital Services Act ("DSA") methodology for determining Very Large Online Platforms ("VLOPs") and Very Large Online Search Engines ("VLOSEs"). But the EU's approach to VLOPs/VLOSEs makes an implicit distinction between services, applying to Online Platforms (as defined in the DSA) and search engines only. Ofcom's definition of "large services," on the other hand, captures *all* types of U2U/search services. As a result, Ofcom's proposed threshold would apply to many different types of services, equating the risk of any in-scope service without further differentiation. We would welcome the opportunity to discuss this complicated issue further and collaborate on a thoughtful threshold to ensure there is predictability for regulated services and consistency in the way regulated regimes are assessing local usage. We would note that even if a service does not meet the threshold amount for a "large service," but somehow possesses a significant risk that deserves additional scrutiny, Ofcom still possesses the power to designate the service for supervision so that it can collaborate on any measurers that may be warranted. We also encourage Ofcom to engage with industry to clarify the methodology regulated services should use when determining the number of monthly active users. The "User numbers" section in Annex 7 for U2U services provides incomplete guidance on how services should count users. (Annex 7 - A11.7 - A11.11). For example, does Ofcom want services to include *all* users or *active* users? If "active," under what circumstances would a user qualify as an "active user?" Annex 8 for search services would similarly benefit from more guidance. Whatever methodology is chosen, we would advocate against aligning to the DSA's methodology for monthly active users ("MAU") for determining designation and for purposes of calculating supervisory fees. We are aware that the European Commission has received a number of informal and formal challenges to its methodology. The variable nature and functions of in-scope services will also impact many variables such as the relevance of daily users versus monthly users, or page views versus engagement. This question may benefit from additional, working discussions with diverse industry participants.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 15:

i) Do you agree with our definition of multi-risk services?

Response: No, the definition should be considered further. Additional nuance could be incorporated to more accurately reflect the relative risk of each regulated service. In the definition's current form, we are concerned it is over-inclusive and could disproportionally apply the most onerous measures to lower risk services.

ii) Please provide the underlying arguments and evidence that support your views.

Response: The definition of "multi-risk" service captures regulated services with medium or high risks that at least *any* two of the 15 illegal harms may occur on the service. But there does not appear to be any data to support the two-harm threshold and we understand Ofcom has acknowledged in other forums that this is to some extent arbitrary, which is reflected in the document's descriptions. The Annex 5 Table 6 risk-levelling guidelines are also written such that almost any risk could potentially be at least medium. For example:

- Likelihood: a medium risk could exist if there is "some evidence of harm" occurring on the service;
- Impact: a medium risk could exist if there is "evidence of harm impacting a material number of users." It is reasonable a service may determine a "material number" is reached once the impact exceeds the low-risk threshold of a "very few" number of users.

The test for the appearance of harm is therefore broad, increasing the likelihood that many, if not most, services may be at risk of multiple harms in some way. This generalized approach could lead to the disproportionate treatment of two services with significantly different risk profiles. For example, a U2U service with a medium risk for two illegal harms with a relatively less severe impact would still be expected to implement the same measures as a U2U service with a high risk for multiple illegal harms.

We believe this result can be avoided if additional levels of differentiation are built into the definition, enabling a more tailored analysis. This could be done in several ways, such as:

- Utilizing the information from Ofcom's risk registers to create a spectrum of approximate impact for the 15 illegal harms. This will avoid treating each of the illegal harms the same and result in a more accurate service risk profile. This could draw on Ofcom's harms research and collaboration with multistakeholder experts.
- Increasing the threshold for medium/high risk illegal harms. In Volume 4 of the consultative materials, Ofcom balances its decision between "at least one kind of illegal harm" and "many kinds of illegal harm," opting for two. Two illegal harms are likely found in most U2U services. We believe a more proportional approach could exist if the threshold were set closer to a middle ground such as seven, for example, or if more objective criteria were added to demonstrate the severity of the harm.
- Integrate additional risk vectors into the definition of "multi-risk" such as service functionality, service-type, or taking into consideration whether a service is a Category 1 or 2a service in the future.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 16:	
i)	Do you have any comments on the draft Codes of Practice themselves?
Response: Please see our responses below on individual Codes of Practice.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 17:	
i)	Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?
Response: No response	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Content moderation (User to User)

Question 18:	
i)	Do you agree with our proposals?
Response: We agree with the proposals and we encourage Ofcom to provide clarity for when a regulated service would meet their obligations under the measure to set and record performance targets.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: We agree that services should have a sufficient amount of flexibility to tailor performance targets so that they are proportionate, given the specific operation of the service. But when would Ofcom determine that a service had failed to set a satisfactory target? Are there operational factors, data or documents Ofcom would expect a service to cite or memorialize when setting its targets?	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Content moderation (Search)

Question 19:
i) Do you agree with our proposals?
Response: No response
ii) Please provide the underlying arguments and evidence that support your views.
Response: No response
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Automated content moderation (User to User)

Question 20:
i) Do you agree with our proposals?
Response: We outline our view on CSAM hash-matching at Questions 22 - 26 below. We acknowledge the thoughtful approach Ofcom has taken to technical proposals and that these have been limited to content that has been communicated publicly on U2U services. However, we are concerned that the current state of technology for CSAM URL matching and fraud keyword detection is insufficient to enable this without risking over-moderation, with potential impacts for fundamental human rights, including the freedom of expression and access to information. It may also result in a significant number of moderation decisions that are overturned on appeal – and likely would require a large increase in the need for human moderation to investigate the open internet for further context. In addition to increasing the wellness risks to these moderators, the length of time required to investigate each case may result in slower resolution of CSAM cases generally. Effectively enabling both types of detection would also require in-scope services to have ongoing and up-to-date access to authoritative sources of information for such URLs and for fraud keywords. While the Internet Watch Foundation currently can provide members with URL lists to support de-listing of CSAM URLs by search engines, we are not aware of any entity providing similar services with respect to fraud.
ii) Please provide the underlying arguments and evidence that support your views.
Response: See above
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 21:

i)	Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?
Response: No response	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Do you have any relevant evidence on:

Question 22:	
i)	Accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;
[✂]	

Question 26:	
i)	An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.
[✂]	
ii)	Please provide the underlying arguments and evidence that support your views.
[✂]	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
[✂]	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

User reporting and complaints (U2U and search)

Question 28:	
i)	Do you agree with our proposals?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Terms of service and Publicly Available Statements

Question 29:	
i)	Do you agree with our proposals?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 30:	
i)	Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Default settings and user support for child users (U2U)

Question 31:	
i)	Do you agree with our proposals?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 32:	
i)	Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?
Response: No response	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 33:	
i)	Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
Response: No response	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Recommender system testing (U2U)

Question 34:	
i)	Do you agree with our proposals?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 35:	
i)	What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response: No response	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive.

Question 36:	
i)	Are you aware of any other design parameters and choices that are proven to improve user safety?
Response: No response	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Enhanced user control (U2U)

Question 37:	
i)	Do you agree with our proposals?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 38:	
i)	Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response: No response	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 39:	
i)	Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Response: No response	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

User access to services (U2U)

Question 40:	
i)	Do you agree with our proposals?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically:

Question 41:	
i)	What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)?
[✂]	
ii)	What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response: See above.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 46:	
i)	Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response: No response	

ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Statutory Tests

Question 48:	
i)	Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard?
Response: Reference is made to our previous responses to Question 14 (definition of large service) and Question 15 (definition of multi-risk service) with regard to assessing the appropriateness of the Codes against the size and type of regulated service (Paragraph 1 of Schedule 4). We would encourage Ofcom to consider our suggestions in each of these responses to ensure the Codes are appropriate to the size and type of regulated service.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: See responses to Questions 14 and 15.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Volume 5: How to judge whether content is illegal or not?

The Illegal Content Judgements Guidance (ICJG)

Question 49:	
i)	Do you agree with our proposals, including the detail of the drafting?
Response: We are supportive and agree with Ofcom's position that a regulated service can alternatively meet its duty to take action against potentially illegal content by applying its own terms of service to that content.	
ii)	What are the underlying arguments and evidence that inform your view?
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response: No response	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Volume 6: Information gathering and enforcement powers, and approach to supervision.

Information powers

Question 52:	
i)	Do you have any comments on our proposed approach to information gathering powers under the Online Safety Act?
Response: We appreciate Ofcom's intended approach of using proportionate means to gather information when necessary, opting for the least intrusive regulatory methods to achieve its goals. We also support Ofcom's methods of obtaining information, like Ofcom's Online Safety Act, Section 104 power to enlist the services of a "skilled person" to assist Ofcom in its duties. However, we believe regulated services could benefit from greater clarity on the qualifications/experience necessary for someone to be approved as a Section 104 "skilled person." Or in the alternative, we would encourage Ofcom to invite the in-scope regulated service to collaborate during the "skilled person" approval process to ensure that the candidate possesses the prerequisite knowledge/experience to understand the service's unique business and content moderation practices to yield a high-quality report.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: See above	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
Response: No response	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Annex 13: Impact Assessments

Question 54:	
i)	Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?
Response: No response	
ii)	If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.
Response: No response	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	