GLOBAL NETWORK INITIATIVE

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: The GNI Principles on Freedom of Expression & Privacy, together with our more detailed Implementation Guidelines (together, “the GNI framework”), as well as the broader, complementary approaches outlined in the UN Guiding Principles on Business and Human Rights (“UNGPs”) and OECD Guidelines for Multinational Enterprises (“OECD Guidelines”), include robust guidance for how companies should conduct due diligence and assess risks associated with human rights. Where such assessments surface actual or potential human rights impacts, the GNI framework helps companies identify steps that they can take to prevent, mitigate, and remedy adverse impacts. These approaches have guided tech company approaches to due diligence and impact assessment for decades and have, in many cases, been deeply woven into the internal governance, systems, and processes of these companies. As such, we recommend that Ofcom explicitly acknowledge and endorse these approaches in its regulations and guidance, and to encourage services subject to the Online Safety Act to refer to them and related, authoritative guidance as they work to implement the OSA’s requirements.

As a general matter, GNI agrees with Ofcom’s assessment that the characteristics of a particular service, as well as its governance, systems, and processes for identifying and addressing risks, contribute significantly to its likelihood of causing impacts on online harms.

ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

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: In this Volume, Ofcom identifies end-to-end encryption and pseudonymity and anonymity as functionalities that “stands out as posing a particular risk” to twelve categories of illegal content: child sexual abuse material, these are: hate crime, terrorism, drugs, immigration, sexual offences, extreme pornography, intimate image abuse, proceeds of crime, fraud, foreign interference and false communications.

While GNI appreciates Ofcom’s recognition that encryption “plays an important role in safeguarding privacy online” and that “[p]seudonymity and anonymity can allow people to express themselves and engage freely online,” as well as its decision to exempt end-to-end encrypted services from certain proposed requirements, we are nevertheless seriously concerned that the framing of these functionalities as broadly posing particular risks may create particular burdens for services that enable them and thereby disincentivize their adoption and deployment across U2U and search services.

GNI therefore strongly recommends that Ofcom remove this framing of encryption as a risk for illegal content and more explicitly acknowledge the significant privacy and security benefits that these functionalities facilitate. In addition, Ofcom should work to articulate clearer guidance on risk mitigation that does not undermine the effectiveness of encrypted technologies and allow services to maintain the benefits of those functionalities while complying with regulation.

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: Ofcom's focus on "governance and accountability processes" as central elements of a service's ability to properly identify and manage online safety risks is consistent with the approaches set out in the GNI framework and the UNGPs and OECD Guidelines.

However, Ofcom also requires all services to name a person accountable to the most senior governance body for compliance with illegal content duties and reporting and complaints duties. GNI has responded to the growing trend of potential liability for company personnel under content regulation in various jurisdictions, noting that without sufficient safeguards and protections, such requirements make it less likely that companies will push back on overbroad government demands or restrictions. Under certain circumstances, senior managers could face administrative or criminal prosecution under the OSA if they fail to comply with an Ofcom information notice. Ofcom should carefully consider what consequences in this context are necessary and proportionate, given the variety of tools that the UK government already has at its disposal to compel compliance.

ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

Response: The second step in Ofcom's proposed "four-step" approach encourages services to "assess risks" by considering the likelihood and potential impact of harms occurring on their services. These align in a general manner with the approach set out in the UNGPs and OECD Guidelines, which focus on the "severity" of potential impacts, which are defined according to the scale, scope, and irremediability of those impacts. GNI encourages Ofcom to acknowledge the concept of "severity" as an important means for prioritizing among risks and to refer explicitly to these factors in its articulation of this approach.

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: GNI acknowledges and supports Ofcom's attempt to broadly align the obligations of internet services to map and mitigate the risks of illegal content with the likelihood and potential impacts of their actual harms using size and risk as separate but interrelated criteria.

However, the range of obligations that apply to smaller, low-risk U2U and search services are nevertheless quite substantial. The costs associated with developing and implementing systems for content moderation, complaints and appeals, risk assessments, and record keeping are individually and collectively substantial. And it is not clear that the costs that these providers will bear, even with guidance and assistance from Ofcom, are justified. These obligations may therefore result in such services taking overly stringent, automated approaches to compliance, which could result in either undercompliance or overcompliance (both of which would have negative impacts on freedom of expression), or avoiding the UK market altogether, which could significantly impact the diversity of services available to UK residents.

These obligations will create significant barriers to entry for new services, those that serve academic, public-interest, and/or non-commercial purposes, and those used and relied upon by communities that are marginalized or associated with particular languages, religions, sexual orientations, or political affiliations.

At a systemic level, such barriers could also substantially limit competition and innovation. For instance, there is an active and ongoing effort globally to federate the storage and management of Internet content in order to empower users and address perceived challenges around content ownership, data protection, and competition. The obligations under the Consultation documents in their present form could create obstacles to these approaches.

It is therefore important for Ofcom to further narrow and tailor obligations under the regulation to appropriate services, paying particular attention to the implications for public interest platforms, smaller/micro businesses, community-led moderation approaches, and internet infrastructure providers.

ii) Please explain your answer.

Response:

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: GNI's company members are required to conduct independent, third-party assessments of their efforts to implement the GNI framework. Those assessments form the basis for GNI's

multistakeholder evaluation of those efforts and resulting recommendations for continuous improvement. GNI has found independent assurance to be a critical component that fosters and facilitates not only our accountability work, but also our shared learning and policy advocacy work. However, independent audit/assurance costs are significant, especially for smaller and medium-sized services, and the thoroughness and credibility of outcomes depend significantly on the methodologies and criteria used, as well as the broader frameworks through which such audits are evaluated. GNI recommends that to the extent that Ofcom considers requiring independent, third-party audits in the future, it should work in collaboration with other regulators, companies, and civil society organizations, international organizations, and multistakeholder initiatives that have experience in this space, to ensure that it builds on and incorporates where appropriate existing, credible practices and experiences.
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:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

Service’s risk assessment

Question 7:
i) Do you agree with our proposals?
Response: As noted above, the GNI framework and other relevant approaches to responsible business conduct focus on human rights due diligence and risk assessment. GNI supports the use of risk assessments as a critical mechanism for identifying and mitigating risks. However, at present, there is no indication in Ofcom’s guidance on whether and when such risk assessments will be made public, either by the services that conduct them or by Ofcom. Transparency with respect to risk assessments would help academics, civil society organizations, and users better understand how services are addressing such risks, and allow them to hold Ofcom accountable for its regulatory obligations.
ii) Please provide the underlying arguments and evidence that support your views.

Response:	
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:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response:	
iv)	Please provide the underlying arguments and evidence that support your views.
Response:	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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: GNI appreciates Ofcom upholding best practices by broadly aligning its approach to developing the illegal content Codes of Practice in line with industry standards. A regulatory approach that emphasizes ensuring that services have the required systems and processes in place to meet their duties, instead of focusing on regulating individual pieces of content, allows different types of companies in the technological stack to develop standards that complement their internal systems and objectives. However, companies may also struggle with the absence of appropriate legal benchmarks in the Consultation, upon which their compliance with content moderation would be assessed by Ofcom. This creates the risk of them often erring on the side of safety (i.e. overcompliance). In addition, the OSA does not cover infrastructure providers (like Cloudflare), but the content they host is a part of the definition of harmful content. Due to such a distinction between direct content providers and infrastructure providers, it is important to recognize that different kinds of services have different abilities to control or moderate content on their platforms.

In a previous submission to the House of Lords, GNI had encouraged lawmakers to avoid broadening the scope of priority illegal content on the Online Safety Bill based on the risk of the overly broad threshold for companies to determine the illegality of content. Under Volume 2 of the current Consultation, however, Ofcom has grouped 130 illegal harms into 15 groups of illegal harm, including hate crime, drugs, terrorism, immigration, intimate image abuse, and fraud. These terms are often global in nature and can be more restrictive than local laws on certain content issues, which creates a general risk of overbroad and/or extraterritorial enforcement.

To ensure that such content is lawfully regulated, GNI acknowledges Ofcom's emphasis on the need for services to develop training schemes on content moderation, as well as its intention to individually supervise the largest and most risky services on content moderation decisions. However, a few concerns remain. For instance, the comprehensive set of documents that set out guidelines from Ofcom on regulating content, albeit useful in several contexts, may also overly burden services - in particular, smaller services with medium to high-risk factors. It also creates unnecessary obstacles to entry for services, especially those intended for academic or non-commercial purposes by individuals or small companies. To avoid this, Ofcom should consider ways to proactively support the implementation of the regulation to protect people from illegal harms in smaller and emerging services.

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

Response:

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:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 14:	
i)	Do you agree with our definition of large services?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 15:	
i)	Do you agree with our definition of multi-risk services?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 16:	
i)	Do you have any comments on the draft Codes of Practice themselves?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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

Content moderation (User to User)

Question 18:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Content moderation (Search)

Question 19:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Automated content moderation (User to User)

Question 20:	
i)	Do you agree with our proposals?
Response: While GNI acknowledges that proactive detection technologies can sometimes be reasonable and efficacious, there remains the concern of over-reliance. This can lead both service providers and regulators to under-appreciate and fail to address deeper challenges and alternative, potentially more rights-aligned solutions to content moderation. In addition, content scanning requirements would seriously undermine and disincentivize the adoption of encrypted technologies. We encourage Ofcom to address risks and potential harms without requiring the use of tools for monitoring communications or proactive detection and removal of broad swathes of user content at risk of legal penalties for noncompliance. However, if these technologies continue to be required, we strongly suggest that Ofcom also require/conduct periodic tests to check their reliability and effectiveness at both the individual service and aggregated levels, with particular attention paid to possible discriminatory impacts; and create an exception for end-to-end encrypted services from obligations to scan content so that these services can continue to make private and secure communications possible.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Bugs in our pockets: the risks of client-side scanning	
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:	

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

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;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 23:	
i)	Ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 24:	
i)	Costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection;;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 25:	

i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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.
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

User reporting and complaints (U2U and search)

Question 28:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Terms of service and Publicly Available Statements

Question 29:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 30:	
i)	Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Default settings and user support for child users (U2U)

Question 31:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 32:	
i)	Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?
Response:	

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

Question 33:	
i)	Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Recommender system testing (U2U)

Question 34:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 35:	
i)	What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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

Enhanced user control (U2U)

Question 37:
i) Do you agree with our proposals?
Response: As a general matter, GNI supports efforts to provide users with enhanced control, which we believe can result in more proportionate and effective measures for addressing online harms and human rights risks. With that said, the costs associated with implementing such measures need to be carefully considered, especially when they are required on the part smaller or non-commercial services.
ii) Please provide the underlying arguments and evidence that support your views.
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:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

Question 39:
i) Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Response:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

User access to services (U2U)

Question 40:

i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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)?
Response:	
ii)	What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 42:	
i)	How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users.

Question 43:	
i)	What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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. Please see our response to Question 4 above.	
ii)	Please provide the underlying arguments and evidence that support your views.
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:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?

Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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: GNI has consistently raised concerns about the outsourcing of enforcement of laws prohibiting content to private companies without appropriate guidance on interpretation and application. We continue to have significant concerns about the possibility, which Ofcom rightly acknowledges, that some covered services will be incentivized to expand their definitions and enforcement of their terms of service to not only include but go beyond the categories of illegal content referenced in the OSA. However, we nevertheless appreciate Ofcom's good faith effort to provide detailed, thoughtful, and "technology-agnostic" guidance through the ICJG.

At the core of our concerns about the OSA's outsourcing of illegal content adjudication, which we flagged during the OSA's legislative process, is the "reasonable grounds to infer" threshold, which Ofcom recognizes is a new and lower threshold than the one used by courts and which we continue to feel is objectively low and is likely to be subjectively applied in different ways by different services and to different users. We acknowledge that this is not a criteria that Ofcom can control at this stage and appreciate Ofcom's emphasis in Volume 5 and Annex 10 on the use of "all relevant information that is reasonably available" by services to identify illegal content, which will be interpreted according to the size and capacity of the service, and whether the service used human moderators or automated systems (or both), which we read as indicative of Ofcom's intention to develop a proportional approach to compliance and enforcement. We also appreciate Ofcom's recognition that processing some of the types of data it defines as constituting "reasonably available information" in the context of judging the illegality of content will have potential implications for users' right to privacy and that services will "need to ensure they process personal data in line with data protection laws."

ii) What are the underlying arguments and evidence that inform your view?

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:

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

Response:

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

Question 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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