Consultation response form

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: Yes, while we support the focus on research and discovery we believe greater engagement with civil society and academia is needed to track emerging threats and identify trends in extremism and disinformation on alt-tech platforms before they emerge in the mainstream. This includes greater support for early career researchers and practitioners who are often on the frontline of monitoring and analysis.	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: We have noticed a trend of emerging threats on alt-tech platforms that do not follow regulation that are rarely recognized by Ofcom and larger enterprise technology firms until they have grown and metastasized. Identifying these trends early and upstream before they reach mainstream platforms and wider audiences is part of a pro-active approach to tracking extremism and disinformation but this requires close and regular engagement with civil society and academia	
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: While we agree with the links between risk factors and different kindof of illegal harms we would seek to expand the range of risk factors that have been identified to include greater emphasis on gender and mental health. The recent literature on these risk factors demonstrates that they are often difficult to identify and quantify but they have significant impact on individuals' trajectories into online harms.	
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: We have concerns about how these proposal will impact free expression and human rights organizations ability to organize protests and dissent online. As currently stated, the proposal risk forcing social media platforms (SMPs) to take action against legitimate, good-faith actors who are dissenting to government policies or views. While the application of these proposals will be critical, we are concerned about the potential for abuse and over-reach. Further scoping and more targeted approaches are recommended.	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: We recommend that the proposals are further scoped and targeted to ensure than civil society, academia, and human rights organizations — as well as individual protestors — are not included. Examples from comparable regulatory proposals in the EU have demonstrated the risks of an overly broad 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: We are in agreement with the types of services the proposals apply to	
ii)	Please explain your answer.
Response: To prevent stifling innovation and entrepreneurship the proposals must be adequately scoped	
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: N/A
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts

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

Service's risk assessment

Question 7:
i) Do you agree with our proposals?
Response: We are concerned about the potential for alt-tech platforms with a significant presence of UK users and no UK-based offices or employees to evade or shirk risk assessments.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We have repeatedly seen smaller, foreign-based alt-tech platforms without a UK, EU, or US presence evade regulation their responsibilities as disinformation and extremism proliferates on their products. While the current proposals do not account for how regulatory measures can reach these platforms, it is of vital importance to ensuring the large sections on the eco-system are safe.
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: Yes
ii) Please provide the underlying arguments and evidence that support your views.

Response: We appreciate the need to observe these regulations in practice but are broadly supportive of the four-step risk assessment process at this stage
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: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response: N/A	
iv)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response: We are supportive of the draft record keeping and review guidance, however it must be adaptable when implemented	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Implementation must be observed over a multi-year period to scope the short-comings and advantages of the guidance	
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: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts	

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: We are concerned about two aspects of the approach proposed. The first relates to protecting human rights advocates, universities and research organizations, and researchers which could be unintentionally affected by the proposal. Further scoping is needed to ensure these actors remain protected and able to continue their work without risk of de-platforming, content removals, or legal risks. Secondly, we emphasis that Ofcom must engage closely and regularly with civil society and academia through an established forum to identify and monitor emerging online harms before they arrive on mainstream platforms.	
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: No, while small platforms should have flexible provisions to support them the classification should be based on the type of platform as well as its size. This ensures that smaller alt-tech platforms are acting responsibly despite only hosting a fracture of the users.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Over the past two years, research outputs from GNET, EGRN, and OxDEL have highlighted the role that small but influential alt-tech platforms play in providing an initial home for extremism and disinformation to expand. An effective Code must take into account these smaller alt-tech platforms (particularly those based outside the UK but with significant users in the UK) and develop measures to bring them into the fold.	
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, while some alt-tech platforms do not classify as large services, they have significantly highly concentrations of malicious actors and/or online harms which risk falling outside the scope of the proposals	

ii) Please provide the underlying arguments and evidence that support your views.
Response: Over the past two years, research outputs from GNET, EGRN, and OxDEL have highlighted the role that small but influential alt-tech platforms play in providing an initial home for extremism and disinformation to expand. An effective Code must take into account these smaller alt-tech platforms (particularly those based outside the UK but with significant users in the UK) and develop measures to bring them into the fold.
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: N/A
ii) Please provide the underlying arguments and evidence that support your views.
Response: N/A
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts

Question 16:
i) Do you have any comments on the draft Codes of Practice themselves?
Response: The proposed Codes of Practice must be more regularly updated to reflect changes in technologies and online harms. As the pace of development can change rapidly over a three month period, the Codes of Practice must be more adaptable and flexible.
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: N/A
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts

Content moderation (User to User)

Question 18:
i) Do you agree with our proposals?
Response: We remain concerned about the free expression of civil society organizations (CSOs), academic researchers, and human rights advocates being curtailed by the existing proposals. While moderation of extremist groups and malicious actors operating on private platforms is necessary and legal, we worry about the scoping of the existing proposal and its potential over-reach or abuse to target legitimate peaceful dissent, civil society and academic researchers. To prevent this, we urge more targeted scoping and clear definitions, along with transparency and a robust appeals process in determining how content is classified and moderated.
ii) Please provide the underlying arguments and evidence that support your views.

Response: Existing examples of risk include individual users, organizations, and researchers who have been caught up for discussing or analysing content which falls outside the narrow bounds of the guidelines. Moreover, when such violations have occurred the appeals process remains unclear, slow, and difficult to navigate. Recent research from Dr Aaron Zelin (Brandeis University) has proposed the development of white-listing certain users or organizations, along with broader solutions that include transparency reports and a robust appeals process.
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: In some cases, search functions continue to recommend content which is extremist but not branded as coming from a designated terrorist organization. As such, the proposals need to better account for the post-organizational structure of extremism with clear definitions of what is permitted and what is not. We remain concerned about the free expression of civil society organizations (CSOs), academic researchers, and human rights advocates being curtailed by the existing proposals. While moderation of extremist groups and malicious actors operating on private platforms is necessary and legal, we worry about the scoping of the existing proposal and its potential over-reach or abuse to target legitimate peaceful dissent, civil society and academic researchers. To prevent this, we urge more targeted scoping and clear definitions, along with transparency and a robust appeals process in determining how content is classified and moderated.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Some content from civil society organizations, researchers, and human rights advocates risks being excluded or downranked. Existing examples of risk include individual users, organizations, and researchers who have been caught up for discussing or analysing content which falls outside the narrow bounds of the guidelines. Moreover, when such violations have occurred the appeals process remains unclear, slow, and difficult to navigate. Recent research from Dr Aaron Zelin (Brandeis University) has proposed the development of white-listing certain users or organizations, along with broader solutions that include transparency reports and a robust appeals process.
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 remain concerned about the free expression of civil society organizations (CSOs), academic researchers, and human rights advocates being curtailed by the existing proposals. While moderation of extremist groups and malicious actors operating on private platforms is necessary and legal, we worry about the scoping of the existing proposal and its potential over-reach or abuse to target legitimate peaceful dissent, civil society and academic researchers. To prevent this, we urge more targeted scoping and clear definitions, along with transparency and a robust appeals process in determining how content is classified and moderated. Automated Content Moderation using AI tools or algorithmic detection further extends these risks and we are concerned that human review will be minimized. Human reviewers bring expertise,

context, and subject matter knowledge that can be missed by automated systems and is important in ensuring that content moderation does not over-step its mandate.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Existing examples of risk include individual users, organizations, and researchers who have been caught up for discussing or analysing content which falls outside the narrow bounds of the guidelines. Moreover, when such violations have occurred the appeals process remains unclear, slow, and difficult to navigate. Recent research from Dr Aaron Zelin (Brandeis University) has proposed the development of white-listing certain users or organizations, along with broader solutions that include transparency reports and a robust appeals process.
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: N/A
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts

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

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

Response: Yes, all parts

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

Question 25:	
i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: We do not work on financial/corporate fraud cases	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts	

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: Industry-wide associations such as the Global Internet Forum for Countering Terrorism (GIFCT) and Tech Against Terrorism are critical for ensuring that hashes from a wide range of platforms and services are included in the database. Strong public-private partnerships are important in ensuring the hash-sharing database is maintained but this must also include smaller platforms which emerge in the future and do not always have access to an in-house Trust & Safety professional. Cryptographic and contextual hashing are helpful to detect 'fuzzy' or approximate hashes however these methods will have to be further improved as Generative Artificial Intelligence (GenAI) applications expand the range of obscuration tools available to extremists and malicious actors seeking to evade automated content moderation. Lastly, the development of a hash database in partnership with academic researchers will help preserve this content for future analysis and enable analysts to flag emerging trends that begin on encrypted platforms to hash-sharing databases.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Hash-sharing is effective but only to the extent the database is continually maintained and updated with new research on extremism and disinformation. The Global Network on Extremism and Technology (GNET) and the Extremism and Gaming Research Network (EGRN) have published significant research on hash-sharing, evasion, and generative artificial intelligence tools which would be helpful in formulating responses.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
Response: When applied to search, automated content moderation has the potential to improve results and filter out harmful content, however we remain concerned about the free expression of civil society organizations (CSOs), academic researchers, and human rights advocates being curtailed by the existing proposals. While moderation of extremist groups and malicious actors operating on private platforms is necessary and legal, we worry about the scoping of the existing proposal and its potential over-reach or abuse to target legitimate peaceful dissent, civil society and academic researchers. To prevent this, we urge more targeted scoping and clear definitions, along with transparency and a robust appeals process in determining how content is classified and moderated. Additionally, greater reliance on trust & safety professionals and academic researchers is recommended to ensure that search results are continually updated to reflect emerging issues and avoid downranking content from legitimate actors advocating for human rights or peaceful political movements.	

ii) Please provide the underlying arguments and evidence that support your views.
Response: When legitimate political dissent or human rights advocacy is removed or downranked in search functions it imperils public trust in automated functions and invites questions surrounding bias and prejudice against particular political movements. To prevent these issues, we urge greater reliance on human experts with subject matter knowledge to train the models and ensure fairness and equal application.
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: We urge the proposals to adopt more robust complaints measures as these are importance both to ensure the fairness of the system and include current information. Teams of subject matter experts can further validate the reports to ensure fairness and accuracy, but these are essential tools to respond fairly and quickly.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Trust in the proposal and platform could be enhanced by ensuring that user reporting and complaints will receive serious consideration. These measures not only reduce perceptions of bias, they can help improve adaptability and accuracy in identifying online harms
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: Yes, we support the proposals' focus on greater clarity and transparency
ii) Please provide the underlying arguments and evidence that support your views.
Response: Improved clarity, standards, and transparency is essential in both improving public trust and enabling academic researchers to access data for further analysis
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: Yes, we urge greater use of the redirect method and pre-bunking initiatives alongside prompts to provide users with reliable information. However we caution that the use of prompts and these tools is only one part of the overall solution as they can be ignored or disregarded, especially with greater exposure to them.
ii) Please provide the underlying arguments and evidence that support your views.
Response: To be effective, prompts and others nudge methods must be continually updated and changed. Moreover, they must use empathy, humour, and serious engagement with disinformation and misinformation to be considered credible by users who are most vulnerable to these online harms. Too often these prompts are generic or worse, condescending and insulting the users they hold to reach and persuade. Insights from behavioural psychology, complex trauma, and education are important to incorporate as these tools become more sophisticated and persuasive.
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: N/A
ii) Please provide the underlying arguments and evidence that support your views.
Response: N/A
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: Yes, all parts

Question 32:	
i)	Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?
Response: N/A	
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: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts	

Recommender system testing (U2U)

Question 34:	
i)	Do you agree with our proposals?
Response: We are strongly supportive of the proposals and encourage greater testing of all products before public release.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Testing and red/blue teaming are essential parts of a safety-by-design approach and we encourage the development of these tools.	
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: Support from industry wide associations and larger platforms which can 'lend' expertise or mentorship to smaller platforms would support the overall health of the ecosystem. Future developments in this field could replicate the success of such programs related to content moderation and trust & safety which have provided smaller companies which lack the resources to ensure they are complying with all regulations.	

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: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts	

Enhanced user control (U2U)

Question 37:	
i)	Do you agree with our proposals?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts	

Question 38:	
i)	Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts	

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

User access to services (U2U)

Question 40:	
i)	Do you agree with our proposals?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts	

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

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

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: N/A	

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

Service design and user support (Search)

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

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: We are sensitive to the burdens placed on small businesses and urge the development of counter-measures to address these challenges. Industry wide associations could lessen the burden on small and micro businesses which lack the resources to comply independently. Additionally, the development of a 'one-stop' office for enquires would further reduce the challenges for small platforms.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Both of these approaches have been successfully applied to other regulatory issues and could be replicated by Ofcom and the Online Safety Bill.
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: We are sensitive to the burdens placed on small businesses and urge the development of counter-measures to address these challenges. Industry wide associations could lessen the burden on small and micro businesses which lack the resources to comply independently. Additionally, the development of a 'one-stop' office for enquires would further reduce the challenges for small platforms.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Both of these approaches have been successfully applied to other regulatory issues and could be replicated by Ofcom and the Online Safety Bill.

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

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

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: N/A	
ii)	What are the underlying arguments and evidence that inform your view?
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response: We are sensitive to the legal and administrative burdens placed on small businesses and urge the development of counter-measures to address these challenges. Industry wide associations could lessen the burden on small and micro businesses which lack the resources to comply independently. Additionally, the development of a 'one-stop' office for enquires would further reduce the challenges for small platforms.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Both of the recommended approaches have been successfully applied to other legal and regulatory issues and could be replicated by Ofcom and the Online Safety Bill.	
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: We urge greater transparency and information sharing, particularly with smaller firms who do not always have access in-house legal advice. This may take the form of a dedicated Ofcom officer role or Ombudsperson but more access to information and analysis should be made available at no-cost to all firms affected.	
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 are concerned about growing information gathering powers under the Online Safety Act. We remain concerned about the free expression of civil society organizations (CSOs), academic researchers, and human rights advocates being curtailed by the existing proposals. While moderation of extremist groups and malicious actors operating on private platforms is necessary and legal, we worry about the scoping of the existing proposal and its potential over-reach or abuse to target legitimate peaceful dissent, civil society and academic researchers. To prevent this, we urge more targeted scoping and clear definitions, along with transparency and a robust audit process that should be continually conducted to determine how much information gathering is necessary.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Creeping advances in information gathering and data collection erode public trust in our legislation and regulatory bodies and have already provoked backlash from civil society and human rights advocates.	
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: We urge the creation of more robust and responsive oversight from elected officials, civil society, and academia on enforcement powers and the Online Safety Enforcement Guidance. This could take the form of a permanent and independent advisory council or a pre-existing body which would expand its mandate. However it is essential that greater oversight is introduced given the sweeping changes and low public trust in the current system.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Greater oversight and transparency on enforcement would improve public trust and perceptions of the enforcement powers while also allowing for mistakes and over-steps to be corrected more quickly.	
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: N/A	
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: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all parts	