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: Overall, we feel this is a comprehensive assessment but that more input is needed in relation to cybercrime and tech-facilitated issues as these appear to be areas which have not been consulted on as widely as some of the other more prominent/ public illegal harms. We would welcome the opportunity to help address this gap through consultancy with The Cyber Helpline	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: Given that your analysis shows that 87% of adult internet users report having encountered a scam or fraud online, we feel this area is missing an analysis of the impact on the service users who experience it. Similarly, a lot is discussed in relation to terrorism, CSAM and exploitation offences but little about stalking and harassment online. At The Cyber Helpline, many cases we deal with on a daily basis related to those involving human behaviour, especially stalking about harassment which account for over 20% of our entire case load. We are working with Ofcom to try and initiate an intelligence-sharing model which could help to provide some of the unique insights that only our service handles and responds to in the UK, which we feel would help to balance out this missing piece.	
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 terms of risk, it's important to note that in the online environment, all users can be considered vulnerable to new and emerging technologies such as AI. An important part of mapping this risk will be ensuring that Ofcom is aware and up to date with the latest trends being seen by front-line services. One risk which is not mentioned in the consultation is that of a user becoming a secondary victim – after initially encountering a form of cybercrime (e.g. doxing, fraud, cyberstalking), then finding the data that has been exposed is used for identity theft or further cyber-enabled crime. There is an opportunity here to appoint the sharing of trends and insights data as part of the super complainant role and to ensure that super complainants appointed cover all areas of illegal harm in the scope of the bill. The Cyber Helpline are well positioned to fulfil this role for cyber and cyber-enabled crime.
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 acknowledge that this is an incredibly difficult area to get right and that there is likely to always be a difference of opinion about both the services in scope and how they are regulated. Whilst we agree in principle, we feel this is going to have to be a work in progress with regular reviews and updates given the huge undertaking of the task	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: There are some areas where we feel some additional factors will need to be considered around tracking new kinds of illegal content and increases in particular kinds of illegal content. This will require adequate resources and capacity for the services in scope to be able to continually monitor and provide meaningful data for change. There is also an opportunity here for NGOs and charities working in the space to provide relevant insight based on the users experiencing issues relating to illegal harm. This will be invaluable data and ensure Ofcom can make informed decisions about the type of accountability measures they take when illegal content codes are breached by services in scope. However, those NGOs and charities will need to, in turn, be adequately resourced to provide the insights required.	
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 feel this is a good starting point but that there is more to do.	
ii)	Please explain your answer.
Response: We acknowledge that this is an incredibly difficult area to get right and that there is likely to always be a difference of opinion about both the services in scope and how they are regulated. Unfortunately, the very nature of regulating services is likely to drive some of the perpetrator behaviour currently being encountered on major platforms onto smaller, less visible services and into dark web spaces, as well as across borders to areas where this bill will not apply, and which understandably cannot be monitored. For this reason, it's vital that as many services as possible are included in scope and consideration is given to the internet being borderless and how the regulator intends to manage this.	

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: It is right that an independent service would review the measures services put in place as they would in any other industry. Further, this right should be passed on to users of the services themselves, and we would call on Ofcom to revisit the Independent Appeals Process campaign led by SWGfL last year when the bill was being debated in the House of Lords and which we fully supported. It makes complete sense for there to be an impartial/ independent body that can mitigate in instances where services in scope have been unable to do so through their own internal reporting mechanisms. We would draw Ofcom's attention to the many Ombudsman services that exist in the UK to help regulate industries from energy and tourism to finance and consumer goods. It makes sense that the same level of regulation should be afforded to the online industry as a whole, and the super complainant role would be a natural place for this to sit.	
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: At The Cyber Helpline, we would like to see such remuneration put back into the services that are currently supporting service users with the very issues those services have failed to address, such as helplines like The Cyber Helpline working to support people who have experienced these issues.	
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: In principle, The Cyber Helpline agrees with the proposals set out but feels there are areas which could be tightened further still
ii) Please provide the underlying arguments and evidence that support your views.
Response: We acknowledge that this is an incredibly difficult area to get right and that there is likely to always be a difference of opinion about both the services in scope and how they are regulated. Unfortunately, the very nature of regulating services is likely to drive some of the perpetrator behaviour currently being encountered on major platforms onto smaller, less visible services and into dark web spaces, as well as across borders to areas where this bill will not apply, and which understandably cannot be monitored. For this reason, it's vital that as many services as possible are included in scope and consideration is given to the internet being borderless and how the regulator intends to manage this. We would like to see all U2U and search services in scope ensure that staff working in content moderation receive training and materials to enable them to identify and take down illegal content. (No 13, 4F). Currently, smaller services in the low and specific risk categories are not covered. Further, these staff are subject to an enhanced DBS and thorough background checks to ensure appropriateness for the role. Once in post, they need to be looked after under a special duty of care to ensure their wellbeing is prioritised by their employers. This would reflect the same level of care and safeguarding we afford our staff and volunteers working at The Cyber Helpline who encounter online harm every day. Section 25 5I notes that there is a dedicated reporting channel for fraud. This is currently only required by large services with a specific risk, but we believe it should be covered by all large services in scope and smaller services that are identified as having a specific risk. The reasoning here is that to be able to properly respond to and prevent this type of harm, we must first be able to fully understand where it is happening. This won't occur if only a minority of services are having to fulfil this obligation. Finally, in the same vein as above, The Cyber Helpline would call for a dedicated reporting channel for all services in scope for all DA-related offences to better track where VAWG is happening to enable a more robust and coordinated 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: 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:

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:	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response: The Cyber Helpline agrees with the guidance and would welcome more specific information from Ofcom about how they intend to monitor and regulate this.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: In the UK, we have allowed services in scope to self-regulate since the invention of the internet, and there is a concern here that just being told to undertake a compliance review once a year will not encourage some services in scope to do so. We feel a more robust monitoring of this requirement will be needed.	
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: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: It's important that all services in scope keep records and review these on a regular basis.	
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: The Cyber Helpline acknowledges that this area is likely to evoke differences of opinion across the sector and that this initial approach is a step in the right direction. We would suggest that the approach itself needs to be reviewed once enforcement has begun to better understand if it is still the right fit, regularly reviewing and amending as required.	
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	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Through the cases handled on the Cyber Helpline, it's often those relating to smaller or more relatively unknown services that can have the highest risk to the user. We have dealt with and responded to high-profile stalking cases where information has been shared on Twitch, Telegram, Snapchat and X, which wouldn't automatically be considered large services in scope but also cases involved from boards and specialist subject fan fiction sites, which will almost always fall into the smaller service category. In our experience working in this space, it's often the biggest players (e.g. Meta and MindGeek) who have done the most already to try and mitigate risks of harm and the smaller sites go relatively unmonitored or regulated in comparison.	
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: As this type of enforcement has never been carried out at this scale globally before it's a bit of an unknown and is a fair starting assumption. As the bill becomes more established, we would recommend regularly reviewing and updating this definition as required.	
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: No

Question 15:
i) Do you agree with our definition of multi-risk services?
Response: As this type of enforcement has never been carried out at this scale globally before it's a bit of an unknown and is a fair starting assumption. As the bill becomes more established, we would recommend regularly reviewing and updating this definition as required.
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: No

Question 16:
i) Do you have any comments on the draft Codes of Practice themselves?
Response: In principle, The Cyber Helpline feels that these codes do not go far enough in terms of who is in scope. We would like to see more of them apply to all services where possible but recognise due to economies of scale that this might be impractical for very small services. Specifically, all governance and accountability measures should be applicable to all services, similarly, content moderation codes relating to CSAM should apply to all services in scope. It is encouraging to see the reporting codes largely being recommended to all services, but we would like to see the 5I dedicated reporting channels put out to all services for Fraud and DA-related illegal harms so that our response as a nation to these crimes and prevention can be better from the start.
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:

Content moderation (User to User)

Question 18:
i) Do you agree with our proposals?
Response: The Cyber Helpline understands the role of Ofcom regulating the services in scope and the fact that it will not be taking a view on individual pieces of online content. We would welcome

further discussion about how then when internal reporting mechanisms of the services in scope fail to address issues, users will find recourse and achieve an effective resolution.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We have concerns that the approach being adopted here amounts to continued self-regulation of the services in scope and that it, therefore, will not have the desired effect to counter harm online and reduce the occurrences of this for users. It Is vital that an independent and impartial appeals process is set up for service users themselves to effectively seek redress for the issues they are facing where services in scope have failed to do this. Currently, under the Video Sharing Platforms regulation, users are afforded this option, and removing that right does not make sense. Further, currently, users who have experienced harm on a UK-based VSP can report this directly to Ofcom through their complaint's mechanism, which won't be the case once the Online Safety Bill is in full force. Where, then, do these users go? Services such as The Cyber Helpline are picking up the shortfall here and providing this much-needed resource for those experiencing cyber and cyber-enabled crime, but we need adequate financial and personnel resources to meet demand as our numbers are only going to get bigger as these regulatory powers come into play. We would welcome further discussion with Ofcom about this.
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: We welcome the requirement for search services in scope to have systems or processes to deindex/ downrank illegal content, but we believe this should be applied to all search services in scope, not just large and multi-risk services. In addition, the comments made in question 18 apply here too.
ii) Please provide the underlying arguments and evidence that support your views.
Response: As detailed in question 18
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 welcome the requirement for U2U services in scope to have URL detection capabilities for CSAM and Fraud content but believe this should be applied to all U2U services in scope, not just large and multi-risk services. In addition, the comments made in question 18 apply here too.
ii) Please provide the underlying arguments and evidence that support your views.
Response: As detailed in question 18
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: The Cyber Helpline agrees with the principles set out in Annex 9 and would just reiterate that regardless of whether a piece of content is deemed private or public in nature if it is shared beyond its initial audience/ outside of its initial purpose it will have the potential to cause harm and the impact of that harm on the individuals experiencing it should be what is being taken into consideration first and foremost here.
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;
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:	

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:	

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:	

Question 25:	
i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
REDACTED [✂]	
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 (i)

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: 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:	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
Response: We welcome the requirement for search services in scope to have URL detection capabilities for CSAM but believe this should be applied to other priority offences, too, such as Fraud. In addition, the comments made in question 18 apply here too.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: As detailed in question 18	
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: The Cyber Helpline are particularly pleased with the detail and scope of the recommendations made in this section for all services in scope. We do believe that there are other trusted flaggers than those mentioned as dedicated reporting channels for Fraud that should also be considered for inclusion. Further, we believe that reporting processes need to be made available to all users, not just those with accounts. Also, the accessibility of these needs to be suited to all users, considering different abilities and neurodivergence.	
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: No	

Terms of service and Publicly Available Statements

Question 29:
i) Do you agree with our proposals?
Response: Yes, we would like to reiterate that the accessibility of these needs to be suited to all users, considering different abilities and neurodivergence.
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: No

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

Default settings and user support for child users (U2U)

Question 31:
i) Do you agree with our proposals?
Response: In principle, The Cyber Helpline agrees with the proposals laid out; however, it would recommend that Ofcom be mindful of the capabilities of age assurance technologies.
ii) Please provide the underlying arguments and evidence that support your views.
Response: The accuracy and bias of age assurance technologies are still relatively unknown, with quite varied levels of response, meaning that this alone cannot be used as an effective way of gauging a user's age. We would recommend that his measure needs to be coupled with others to help identify child users and ensure that all children are properly protected on the services in scope.
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: We would recommend exploring if the default settings for push prompts encouraging users to engage with more content of a similar nature could be disabled for children to help with the management of their online experience	
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:	

Recommender system testing (U2U)

Question 34:	
i)	Do you agree with our proposals?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Too often, services in scope have separate safety and development teams, meaning that product developments currently don't always receive the robust signoff with due consideration to user safety that they should. We would recommend consulting with Roblox about their unique approach to product development sign-offs, ensuring that safety is at the heart of this as a potential best practice model for other services to replicate.	
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: As mentioned above, the Roblox process to overcome this could be a best practice example for other smaller services to follow.	
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: Yes – Mind Geek proactively alert users when they search for illegal content on their services alerting them why they cannot find this and giving them a prompt to seek help for this behaviour through Stop it Now in the UK. Also, they proactively remove content when it is reported, operating a remove first, then investigating and reinstating, if need be, meaning minimal risk of additional exposure to harmful content once it has been reported. This is a best practice example that other mainstream services should adopt for illegal content. In addition, signing up for StopNCII is a way to proactively prevent a service from sharing non-consensual intimate image abuse material. This should be a requirement for all platforms in scope to address image-based sexual abuse on their platforms.	
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: Yes – further, designs on Meta and X services allow users to turn comments off on posts and to ban certain words from appearing in their feeds to prevent certain abuse from appearing.	
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: 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: Yes	
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: The Cyber Helpline recognises that it would be useful to understand the credibility of the information being consumed by the user, and labelling accounts through voluntary verification schemes is an equally transparent way of doing this. We would recommend that this does not become a paid subscription-based verification, however, as this undermines the authenticity of the verification (e.g. X and Meta's ticks subscription services).	
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: Yes – we feel this should be expanded to other illegal priority offences, too, and not just limited to CSAM. Due consideration needs to be given to how the content is shared, however, as it's widely recognised that a proportion of this type of content is often circulated through inauthentic accounts, meaning that innocent users could be held responsible for actions in which they had no part.	
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: 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)?
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:	

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: N/A	
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: N/A	
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: Yes – We would recommend consulting with Roblox about their unique approach to product development sign-offs, ensuring that safety is at the heart of this as a potential best practice model for other services to replicate.	
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: 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 – As detailed earlier in this response, in our experience it is often the smaller services and relatively unknown players where the most risk of harm is, largely due to ineffective content moderation and minimal to no trust and safety mechanisms on the services. For this reason, it is our feeling that these services need to be helped to be held accountable, perhaps in a buddy style system with larger services in scope	
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: 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 – as detailed above in question 45	
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: No	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services is proportionate?
Response: Yes, in principle	
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: 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: Yes, in principle	
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: 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: In principle, yes. It is likely that this will evolve as regulatory powers come into force, and it may need reviewing and updating as appropriate, but this provides a good starting point.	
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: No	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response: Yes. The Cyber Helpline wonders if there may be scope within Ofcom's regulatory powers to advise smaller services of pro bona legal support they may be able to access in this regard, where necessary.	
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: No	

Question 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response: N/A	
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: No	
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: No	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
Response: Not of significant note, only that we would recommend that enforcement is taken promptly in relation to illegal content as it is likely that the breaches made will cause significant risk of harm for the service users.	
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: 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:	