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	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: Yes – see my two page "Illegal Harms Consultation - Response from SafeCast"	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No – However my paper "A Response to 'Thoughts on Child Safety on Commodity Platforms_ by Dr Ian Levy and Crispin Robinson' contains material which might be termed "sensitive" from Page 4 onwards. That paper was sent to GCHQ in November 2022.	

Question 2:	
i)	Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.
Response: No	
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: Yes	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: See the evidence re DMCA take-downs based on fake websites reported by Tax Policy Associates and our two page "Illegal Harms Consultation - Response from SafeCast"	
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: Yes	
ii)	Please explain your answer.
Response: Ofcom's proposals are proportionate	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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: Yes – See our 2022 paper " "Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill" as well as our additional comments below	
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: No	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Service's risk assessment

Question 7:	
i)	Do you agree with our proposals?
Response: Generally yes but subject to the caveat that they are somewhat bureaucratic and hinders new entrants	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: See our 2022 paper " "Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill" as well as our additional comments below	
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 so long as it does not stop new entrants	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: See our 2022 paper " "Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill" as well as our additional comments below	
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: Yes so far as they go
ii) Please provide the underlying arguments and evidence that support your views.
Response: Insufficient consideration is being given to the long term risks arising from “bad actors” keeping and using images and records of communications made by children when they are children.
iii) Do you think the information provided on risk factors will help you understand the risks on your service?
Response: The information on risk factors is helpful so far as it goes
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: No

Record keeping and review guidance

Question 10:
i) Do you have any comments on our draft record keeping and review guidance?
Response: Consideration should be given to the appointment of an external auditor to report to Ofcom in respect of the largest social media companies in a similar way to the audit of public limited companies under the Companies Acts
Please provide the underlying arguments and evidence that support your views.
Response: The use of independent external audit with a mandated reporting requirement to Ofcom should stop social media companies from fabricating false records if it were properly policed. Recent fraud cases (WorldCom; Enron) raise the importance of independent external audit as a control measure.
a. 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: The bureaucratic burden is very heavy. Please consider our 2022 paper " "Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill" as well as our additional comments below as means to reduce the implementation costs
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: No	
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: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: The bureaucratic burden is very heavy. Please consider our 2022 paper " "Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill" as well as our additional comments below as means to reduce the implementation costs	
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: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: The bureaucratic burden is very heavy. Please consider our 2022 paper " "Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill" as well as our additional comments below as means to reduce the implementation costs	
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: Yes
ii) Please provide the underlying arguments and evidence that support your views.
Response: The bureaucratic burden is very heavy. Please consider our 2022 paper " "Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill" as well as our additional comments below as means to reduce the implementation costs
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: No
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: The bureaucratic burden is very heavy. Please consider our 2022 paper " "Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill" as well as our additional comments below as means to reduce the implementation costs
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Content moderation (User to User)

Question 18:
i) Do you agree with our proposals?
Response: Yes
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

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: No – See: my paper "A response to "Thoughts on Child Safety on Commodity Platforms_ by Dr Ian Levy and Crispin Robinson"	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Metadata labelling if done in accordance with a global standard can enable the quick and effective removal of potentially harmful content without censorship through the use of lightweight filters. This would greatly reduce the areas which the security services and the NCA need to actively police and review content . It is also the only way in which there could be an effective UK "*CyberTipline"* service which adhered to Ofcom transparency and openness requirements given the numbers involved Furthermore the need for "*Outcome21"* peer to peer protections, so that children are not criminalised for just being curious and social amongst their peers, can only be implemented in accordance with global standards. Client side protections require economies of scale which can only be deployed in accordance with a standard that does not create commercial barriers to new entrants or protected silos for the incumbents. Failure to implement these measures could also result in some long tail risks as youthful behaviour resurfaces from web archives in a child's adult life - this has already been identified as a long term security risk by unfriendly foreign state actors building dossiers for blackmail at a future time.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 21:	
i)	Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?
Response: No	

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: This is feasible if done in association with metadata labelling using SafeCast HeadCodes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: SafeCast's proposals set out in the paper "*Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill*" makes the case for the use of SafeCast HeadCodes as metadata labels in video content. This would greatly reduce the volume of data which would need to be reviewed under Hash matching and URL detection for terrorism content (Automated Content Moderation Proposals) - Effectively leaving these actions to be undertaken only on content on the Dark Web and hence away from day-to-day contact with children and vulnerable people who would be protected by lightweight filters in their mobile devices. In view of the fact that SafeCast's HeadCodes have been accepted by the Society for Motion Picture and Telecommunications Engineers (SMPTE) as being part of new SMPTE digital standards, it is possible that major Child Sex Abuse Materials (CSAM) elimination measures could be implemented without censorship via the early implementation of SafeCast HeadCodes as Self Applied Content Ratings to be included whenever any video is uploaded (as was requested by the DCMS in 2016 and in the Joint Position of the NPCC and the National Crime Agency (**NCA**) in Chief Constable Simon Bailey's evidence to the Home Affairs Select Committee in 2018. At this time Simon Bailey was the lead for Child Protection at the National Police Chief Council (**NPCC**).	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

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: This is feasible if done in association with metadata labelling using SafeCast HeadCodes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: SafeCast's proposals set out in the paper "*Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill*" makes the case for the use of SafeCast HeadCodes as metadata labels in video content. This would greatly reduce the volume of data which would need to be reviewed under Hash matching and URL detection for terrorism content (Automated Content Moderation Proposals) - Effectively leaving these actions to be undertaken only on content on the Dark Web and hence away from day-to-day contact with children and vulnerable people who would be	

protected by lightweight filters in their mobile devices. In view of the fact that SafeCast's HeadCodes have been accepted by the Society for Motion Picture and Telecommunications Engineers (SMPTE) as being part of new SMPTE digital standards, it is possible that major Child Sex Abuse Materials (CSAM) elimination measures could be implemented without censorship via the early implementation of SafeCast HeadCodes as Self Applied Content Ratings to be included whenever any video is uploaded (as was requested by the DCMS in 2016 and in the Joint Position of the NPCC and the National Crime Agency (**NCA**) in Chief Constable Simon Bailey's evidence to the Home Affairs Select Committee in 2018. At this time Simon Bailey was the lead for Child Protection at the National Police Chief Council (**NPCC**).

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

Response: No

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: Metadata labelling using SafeCast HeadCodes could move all CSAM URL detection requirements to be reserved solely for the Dark Web

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

Response: SafeCast's proposals set out in the paper "*Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill*" makes the case for the use of SafeCast HeadCodes as metadata labels in video content. This would greatly reduce the volume of data which would need to be reviewed under Hash matching and URL detection for terrorism content (Automated Content Moderation Proposals) - Effectively leaving these actions to be undertaken only on content on the Dark Web and hence away from day-to-day contact with children and vulnerable people who would be protected by lightweight filters in their mobile devices. In view of the fact that SafeCast's HeadCodes have been accepted by the Society for Motion Picture and Telecommunications Engineers (SMPTE) as being part of new SMPTE digital standards, it is possible that major Child Sex Abuse Materials (CSAM) elimination measures could be implemented without censorship via the early implementation of SafeCast HeadCodes as Self Applied Content Ratings to be included whenever any video is uploaded (as was requested by the DCMS in 2016 and in the Joint Position of the NPCC and the National Crime Agency (**NCA**) in Chief Constable Simon Bailey's evidence to the Home Affairs Select Committee in 2018. At this time Simon Bailey was the lead for Child Protection at the National Police Chief Council (**NPCC**).

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

Response: No

Question 25:

i) Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;

Response: Metadata labelling using SafeCast HeadCodes could move all CSAM URL detection requirements to be reserved solely for the Dark Web
ii) Please provide the underlying arguments and evidence that support your views.
Response: SafeCast's proposals set out in the paper "*Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill*" makes the case for the use of SafeCast HeadCodes as metadata labels in video content. This would greatly reduce the volume of data which would need to be reviewed under Hash matching and URL detection for terrorism content (Automated Content Moderation Proposals) - Effectively leaving these actions to be undertaken only on content on the Dark Web and hence away from day-to-day contact with children and vulnerable people who would be protected by lightweight filters in their mobile devices. In view of the fact that SafeCast's HeadCodes have been accepted by the Society for Motion Picture and Telecommunications Engineers (SMPTE) as being part of new SMPTE digital standards, it is possible that major Child Sex Abuse Materials (CSAM) elimination measures could be implemented without censorship via the early implementation of SafeCast HeadCodes as Self Applied Content Ratings to be included whenever any video is uploaded (as was requested by the DCMS in 2016 and in the Joint Position of the NPCC and the National Crime Agency (**NCA**) in Chief Constable Simon Bailey's evidence to the Home Affairs Select Committee in 2018. At this time Simon Bailey was the lead for Child Protection at the National Police Chief Council (**NPCC**).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

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: Metadata labelling using SafeCast HeadCodes could move all CSAM URL detection requirements to be reserved solely for the Dark Web
ii) Please provide the underlying arguments and evidence that support your views.
Response: SafeCast's proposals set out in the paper "*Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill*" makes the case for the use of SafeCast HeadCodes as metadata labels in video content. This would greatly reduce the volume of data which would need to be reviewed under Hash matching and URL detection for terrorism content (Automated Content Moderation Proposals) - Effectively leaving these actions to be undertaken only on content on the Dark Web and hence away from day-to-day contact with children and vulnerable people who would be protected by lightweight filters in their mobile devices. In view of the fact that SafeCast's HeadCodes have been accepted by the Society for Motion Picture and Telecommunications Engineers (SMPTE) as being part of new SMPTE digital standards, it is possible that major Child Sex Abuse Materials (CSAM) elimination measures could be implemented without censorship via the early implementation of SafeCast HeadCodes as Self Applied Content Ratings to be included whenever any video is uploaded (as was requested by the DCMS in 2016 and in the Joint Position of the NPCC and the National Crime Agency (**NCA**) in Chief Constable Simon Bailey's evidence to the Home Affairs Select Committee in 2018. At this time Simon Bailey was the lead for Child Protection at the National Police Chief Council (**NPCC**).
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: Metadata labelling using SafeCast HeadCodes could move all CSAM URL detection requirements to be reserved solely for the Dark Web
ii) Please provide the underlying arguments and evidence that support your views.
Response: SafeCast's proposals set out in the paper "*Some measures to improve the effectiveness, enforceability and universality of the UK Online Safety Bill*" makes the case for the use of SafeCast HeadCodes as metadata labels in video content. This would greatly reduce the volume of data which would need to be reviewed under Hash matching and URL detection for terrorism content (Automated Content Moderation Proposals) - Effectively leaving these actions to be undertaken only on content on the Dark Web and hence away from day-to-day contact with children and vulnerable people who would be protected by lightweight filters in their mobile devices. In view of the fact that SafeCast's

HeadCodes have been accepted by the Society for Motion Picture and Telecommunications Engineers (SMPTE) as being part of new SMPTE digital standards, it is possible that major Child Sex Abuse Materials (CSAM) elimination measures could be implemented without censorship via the early implementation of SafeCast HeadCodes as Self Applied Content Ratings to be included whenever any video is uploaded (as was requested by the DCMS in 2016 and in the Joint Position of the NPCC and the National Crime Agency (**NCA**) in Chief Constable Simon Bailey's evidence to the Home Affairs Select Committee in 2018. At this time Simon Bailey was the lead for Child Protection at the National Police Chief Council (**NPCC**).
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:
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: Yes	
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:	
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 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:	
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 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:	
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:	

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:	