

## Your response

### Volume 2: The causes and impacts of online harm

#### Ofcom's Register of Risks

Question 1:	
i)	Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?
Response:  The assessment is thorough and methodological. Easy to understand and it identifies the inherent risks in the business models is sets out to examine.	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: No	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 2:	
i)	Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.
Response: No. The links are correct.	
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: No

- 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: The scope of services that you are describing is adequate. I might suggest that you assess whether the level of granularity with respect to the size of businesses and the required measures could be simplified.

- 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: No. Third party assurance may be warranted for larger platforms, or platforms whose controls or enforcement actions have been found lacking. Obligatory third party assurance is not warranted for all entrants.

- 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: I am not aware of any direct evidence but it seems a reasonable suggestion to ensure execs and managers gives sufficient attention and monitor online safety outcomes.

- 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: Yes

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

Response: The suggested risk assessment methodology (steps and profiles) is comprehensive and it addresses the right universe of issues relating to potential harm. Applying this approach will achieve two important outcomes: correct identification of risks associated with services and, secondly, an appropriate and necessary focus on controls to minimise harmful outcomes to materialise.

- 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: See question 7

- 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

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

Response: The risk profiles are adequate in that they provide both analytical clarity in distinguishing between different services and sufficiently detail in describing activities and functional aspects of each service

iii) Do you think the information provided on risk factors will help you understand the risks on your service?

Response: Yes

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

Response: The information will be particularly valuable to third parties providing technology and other services to service providers, and the risk profiles will also help smaller players to perform risk assessments of their business models and design appropriate controls.

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

Response: No

## Record keeping and review guidance

**Question 10:**

i) Do you have any comments on our draft record keeping and review guidance?

Response: No.

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

Response: Guidance and proposals are clear.

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: There is no good justification why any service provider should be exempt from these requirements.

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: These measures are reasonable and commensurate with requirements stipulated by international payments schemes

- 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: Controls should be commensurate to inherent risks be they by impact or instance

- 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: Aligned to the DSA (EU)

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

Response: No

<b>Question 15:</b>	
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: It will ensure that appropriate controls are designed to protect from specific harms	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

<b>Question 16:</b>	
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	

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

## Content moderation (User to User)

<b>Question 18:</b>	
i)	Do you agree with our proposals?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: The proposals are in line with existing business and assurance practices employed by established players and required by international payment schemes.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

## Content moderation (Search)

<b>Question 19:</b>	
i)	Do you agree with our proposals?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Proposed measures are a reasonable preventative control	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

## Automated content moderation (User to User)

<b>Question 20:</b>	
i)	Do you agree with our proposals?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: The proposed measures are in line with industry best practice and the technology and providers are readily available.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

<b>Question 21:</b>	
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:***

<b>Question 22:</b>	
i)	Accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;
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

<b>Question 23:</b>
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: 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

<b>Question 24:</b>
i) Costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection;;
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

<b>Question 25:</b>
i) Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
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

**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: 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

## Automated content moderation (Search)

**Question 27:**

- i) Do you agree with our proposals?

Response: Yes

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

Response: Proposed measures are in line with best practice in control assurance deployed by large players and technology is available.

- 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: Yes

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

Response: It is proportionate for larger or higher risk service provider to use the user reporting and complaints channels as part of their overall detective control framework and as an additional check on other controls for detection and learning purposes.

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

Question 30:	
i)	Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response: No	
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	

## Default settings and user support for child users (U2U)

Question 31:	
i)	Do you agree with our proposals?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: The proposed measures seem reasonable to help protect children and help them help themselves	
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: Not my area of expertise	

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

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

## Recommender system testing (U2U)

<b>Question 34:</b>
i) Do you agree with our proposals?
Response: Yes
ii) Please provide the underlying arguments and evidence that support your views.
Response: Measures provide an extra layer of controls and checks
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

<b>Question 35:</b>
i) What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response: None
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.***

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

Response: No
--------------

## Enhanced user control (U2U)

<b>Question 37:</b>
---------------------

i) Do you agree with our proposals?
-------------------------------------

Response: Yes
---------------

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

Response: Provides extra protection and should also be coupled with information on how to report content
--

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

Response: No
--------------

<b>Question 38:</b>
---------------------

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
--------------

<b>Question 39:</b>
---------------------

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: No
--------------

## User access to services (U2U)

<b>Question 40:</b>
---------------------

i) Do you agree with our proposals?
-------------------------------------

Response: Yes
---------------

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

Response: Measures seem proportionate and reasonable
--

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: No

- ii) What are the advantages and disadvantages of the different options, including any potential impact on other users?

Response: No

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

Response: NO

**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: If a categorisation of the infraction severity exists this may make sense in the case of 'mistakes' or borderline cases but in general my view is that verified CSAM dissemination by a user should disqualify that user permanently.

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

Response: No

***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: Institute an appeals process

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

Response: No

## Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: The measures are effective preventive controls	
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: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: It is the risk of harm that must be addressed not the service provider's ability to design and implement controls	
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: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: It is the risk of harm that must be addressed not the service provider's ability to design and implement controls	
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: Yes
ii) Please provide the underlying arguments and evidence that support your views.
Response: Larger service providers are already deploying resources to provide controls and compliance assurance
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

## Statutory Tests

<b>Question 48:</b>
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
ii) Please provide the underlying arguments and evidence that support your views.
Response: The recommendations take account of the principles that the statute requires
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: Yes

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

Response: The guidelines are in line with existing compliance requirements and policy positions taken by NGOs

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

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: Adequate

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: 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: 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	

## Annex 13: Impact Assessments

<b>Question 54:</b>	
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: Yes	
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: No	