Your response

Question (Volume 2)	Your response
Question 6.1: Do you have any comments on Ofcom's assessment of the causes and impacts of online harms? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.	We have no comments.
Question 6.2: 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.	*Is this answer confidential? No* The current model seems to consider risk factors in isolation without taking into account appropriate controls. We propose that the model distinguishes between mitigated and unmitigated risks. For example, livestreaming should be a risk factor if it is offered without corresponding mitigating measures. In relation to all illegal harms, but in particular CSEA and CSAM, we would encourage Ofcom to consider whether tag or keyword-based search discoverability (as opposed to only specific 'user search') should be considered a functionality-based risk factor.

Question (Volume 3)	Your response
Question 8.1: Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice? Please provide underlying arguments and evidence of efficacy or risks to support your view.	*Is this answer confidential? No* Yes.

Question (Volume 3)	Your response
Question 8.2: Do you agree with the types of services that we propose the governance and accountability measures should apply to?	*Is this answer confidential? No* Yes.
Question 8.3: 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?	*Is this answer confidential?* **Mixed response** *This portion of our answer is non-confidential:* Yes, although an audit must be independent and tailored to the specific risks associated with each online service. █████████ already instructs an independent third party, which we call a "Monitor", to assess and validate the design, implementation, and effectiveness of our compliance program. The appointment of the Monitor comes at a substantial financial cost and requires significant time from senior leaders at ████████. ████████████████████████ ███████████████████████████████ █████████████████
Question: 8.4: 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?	*Is this answer confidential? No* "Positive online safety outcomes" is an undefined term which would be difficult to accurately measure in practice. We are not aware of any research-backed evidence supporting this measure.
Question 9.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Yes. We encourage Ofcom to define 'high impact' users as active users within the prior 6 months, and to use this metric for defining a 'large service'. This aligns Ofcom guidance and the EU Digital Services Act.

Question (Volume 3)	Your response
Question 9.2: 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?	*Is this answer confidential? No* Yes. At Step 1, we encourage Ofcom to outline the importance of recording where a functionality has been newly introduced which may lead to a new risk factor (e.g. end-to-end encryption).
Question 9.3: Are the Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service?[1]	*Is this answer confidential? No* Yes. There is a typo/missing word on page 64 of Volume 3 in the sentence that begins with "would need to provide…" which requires clarification. The relevant paragraph is: *"This approach does require services to self-select relevant risk factors. To limit ambiguity or confusion, we have provided services with a draft glossary. would need to provide a linked glossary"*
Question 10.1: Do you have any comments on our draft record keeping and review guidance?	*Is this answer confidential? No* We request clarification on the 'named responsible person for overseeing the [risk assessment/process]'. Must this be the same person who is responsible for a) compliance with an Information Notice in Chapter 28 and/or b) compliance with illegal content duties and reporting and complaints duties in Chapter 8? We would also welcome guidance on the level of seniority required, any domicile requirements, and whether an individual would be responsible for all online safety risk assessments or specific categories (i.e. CSEA vs Financial Risks).
Question 10.2: 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?	*Is this answer confidential? No* Yes.

---

[1] If you have comments or input related the links between different kinds of illegal harm and risk factors, please refer to Volume 2: Chapter 5 Summary of the causes and impacts of online harm).

Question (Volume 4)	Your response
Question 11.1: Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?	*Is this answer confidential? No* We ask that Ofcom consider the definitions already adopted by other legal and regulatory regimes since most online services operate internationally. We also suggest that the age of users (and target user groups) be a material factor when considering risk profiles.
Question 11.2: 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?	*Is this answer confidential? No* We agree and note that the age of users (and target users) should be a material factor when considering risk profiles.
Question 11.3: Do you agree with our definition of large services?	*Is this answer confidential? No* As above, we suggest that the user base calculation is made consistent with the EU Digital Services Act and is based on active users.
Question 11.4: Do you agree with our definition of multi-risk services?	*Is this answer confidential? No* Yes
Question 11.6: Do you have any comments on the draft Codes of Practice themselves?[2]	*Is this answer confidential? No* No.
Question 11.7: Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?	*Is this answer confidential? No* No.

---

[2]   See Annexes 7 and 8.

Question (Volume 4)	Your response
Question 12.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* We would welcome the inclusion of a specific section dedicated to 'Safety by Design'.
Question 13.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Not Applicable.
Question 14.1: Do you agree with our proposals? Do you have any views on our three proposals, i.e. CSAM hash matching, CSAM URL detection and fraud keyword detection? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Yes. We would also support a requirement for key-word detection for CSAM/CSEA risks.
Question 14.2: Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?	*Is this answer confidential?* **Mixed response** *This portion of our answer is not confidential*: We would welcome further clarification from Ofcom on when content would be considered to be communicated privately vs publicly. ██████████████████ ████████████████████ ████████████████████████ ███████████████████████ ██████████████████ ████████████████████████ ███████████████████████ ██████████████████ ██████████████████████ █████████████████ ██████

Question (Volume 4)	Your response
Question 14.3: Do you have any relevant evidence on: ● The accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services; ● The 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; ● The costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching[3] for CSAM URL detection; ● The costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services; and ● 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.	*Is this answer confidential? No* No.

---

[3]   Fuzzy matching can allow a match between U2U content and a URL list, despite the text not being exactly the same.

Question (Volume 4)	Your response
Question 15.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Not Applicable.
Question 16.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Yes. However we request clarification on the question of whether Ofcom will provide a list of trusted flaggers only with respect to fraud or whether Ofcom will provide a list of trusted flaggers for more (or all) harms.
Question 17.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Yes and we would welcome clarification that the age of the users (or target group of users) will determine what language and style is appropriate for a service's Terms of Service.
Question 17.2: Do you have any evidence, in particular on the use of prompts, to guide further work in this area?	*Is this answer confidential? No* No.
Question 18.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Not Applicable.
Question 18.2: Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?	*Is this answer confidential? No* Not Applicable.

Question (Volume 4)	Your response
Question 18.3: Are there other points within the user journey where under 18s should be informed of the risk of illegal content?	*Is this answer confidential? No* Not Applicable.
Question 19.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Not Applicable. ▇▇▇▇▇ does not have relevant recommender systems on the platform.
Question 19.2: What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?	*Is this answer confidential? No* Not Applicable. ▇▇▇▇ does not have relevant recommender systems on the platform.
Question 19.3: 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. Are you aware of any other design parameters and choices that are proven to improve user safety?	*Is this answer confidential? Yes* ▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇ ▇▇▇▇▇▇▇▇▇▇▇▇▇ ▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇ ▇▇▇▇▇▇▇▇▇▇▇▇ ▇▇▇▇▇▇▇▇▇▇▇▇▇ ▇▇▇▇▇▇▇
Question 20.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Yes.

Question (Volume 4)	Your response
Question 20.2: Do you think the first two proposed measures should include requirements for how these controls are made known to users?	*Is this answer confidential? No* Yes.
Question 20.3: Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?	*Is this answer confidential? Yes* ███████████████████████████ ███████████████████████████
Question 21.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Yes.
Question 21.2: Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically: ● 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)? What are the advantages and disadvantages of the different options, including any potential impact on other users? ● How long should a user be blocked for sharing known CSAM, and should the period	*Is this answer confidential? Yes* ████████████████████████████ █████████████████████████████ ██████████████████████████ ████████████████████████ ██████████ ███████████████████████████ ████████████████████████████ ████████████████████████████ ██████████████████████████ ███████████████████████████ ██████████████████████████ ██████████████████████████ ██████ ███████████████████████████ ██████████████████████████ ██████████████████████████ ██████████████████

Question (Volume 4)	Your response
vary depending on the nature of the offence committed? ● 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. 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?	
Question 22.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*Is this answer confidential? No* Not Applicable.
Question 23.1: Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?	*Is this answer confidential? No* Not Applicable.
Question 23.2: 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?	*Is this answer confidential? No* Not Applicable.

Question (Volume 4)	Your response
Question 23.3: We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?	*Is this answer confidential? No* We support a risk based approach to online safety.
Question 24.1: 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? If not, why not?	*Is this answer confidential? No* Yes.

Question (Volume 5)	Your response
Question 26.1: Do you agree with our proposals, including the detail of the drafting? What are the underlying arguments and evidence that inform your view.	*Is this answer confidential? No* Yes.
Question 26.2: Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?	*Is this answer confidential? No* No. We consider that an understanding of regulatory law and/or the legislative process is necessary to understand the Ofcom guidance.
Question 26.3: What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?	*Is this answer confidential? No* Not Applicable.

Question (Volume 6)	Your response
Question 28.1: Do you have any comments on our proposed approach to information gathering powers under the Act?	*Is this answer confidential? No* We welcome the provision of a proposed timeline in advance of Information Notices to enable resources to be allocated accordingly. The cadence, volume, density, and length of Information Notices should be carefully considered to ensure Services can allocate resources to comply with information gathering exercises while maintaining focus on preventing online harms. In order to enable Services to balance these obligations, we suggest: - An advance timeline of Information Act cadence (including draft publication, final notice publication and response deadline); - Effecting a cadence that does not result in multiple Information Notices sent to Services at the same time; - Allowing sufficient time to respond and inviting early extension applications from Services if resourcing or external factors render the deadline unachievable; - Avoiding repeating questions from previous Information Notices or Calls for Evidence. In the event this is impractical, we would invite Ofcom to explicitly allow Services to re-submit previous responses and flag they are doing so to Ofcom in its Information Notice response.
Question 29.1: Do you have any comments on our draft Online Safety Enforcement Guidance?	*Is this answer confidential? No* No.

Question (Annex 13)	Your response
Question A13.1: Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record	*[Is this answer confidential? No* Not Applicable.

Question (Annex 13)	Your response
keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?	
Question A13.2: 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.	*Is this answer confidential? No* Not Applicable.

Please complete this form in full and return to IHconsultation@ofcom.org.uk.