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.	[Is this answer confidential? No] Ofcom should ensure that providers are aware that laws in relation to illegal harms may vary in the devolved nations and refer them to the relevant section of the Online Safety Act 2023 ("the 2023 Act"). For example, child sexual abuse and exploitation ("CSAE") offences in the 2023 Act differ in Scotland from the rest of the UK. Also, not all of the offences created by the 2023 Act are being introduced in Scotland, for example the false and threatening communications offences. At Section 6C.4, Volume 2, there is reference to 'self-generated indecent images (SGII)'. This is not a term used in Scotland by Government or Police Scotland; rather, the term 'self-generated Child Sexual Abuse Material' is used. This, and other terminology which differs between UK jurisdictions should be reflected in any analysis or guidance for providers. At Section 6C.6, Volume 2, a definition of CSAE is given but this does not set out the age threshold for a child or young person. Ofcom should set out clear age thresholds to ensure there is clarity for providers. Ofcom should ensure that providers are clear on the risk of peer on peer and under-18 CSAE-related activity using online platforms. Hackett (2004), in review of the pattern of crime statistics over a decade, estimated that between one fifth and one third of all child sexual abuse ("CSA") in the UK involves under-18s as the child who has harmed. (Hackett, 2004, What Works for Children and Young People with Harmful Sexual Behaviours.) Gerwitz-Meydan and Finkelhor (2019), in a study of a sample of 0-17-year-olds in the USA found that 70% of CSA offences against girls and 77% of CSA offences against boys were perpetrated by an under-18. (Gewirtz-Meydan, Finkelhor, 2019, 'Sexual Abuse and Assault in a Large National Sample of Children and Adolescents'.) Ofcom should consider additional guidance on groups who are at risk, but may not have the digital skills to access or understand protective measures – e.g. the elderly,

Question (Volume 2)	Your response
	learning disabled, neurodiverse or those living in digital poverty with restricted services or access. We have some concern around the grouping of unlawful migration and human trafficking. Individuals resident in the UK are also susceptible to online harms, including human trafficking. This could be made clearer. Providers will need to have clear guidance differentiating between the offence of human trafficking in Scotland under the Human Trafficking and Exploitation (Scotland) Act 2015 (HTE) and the offence of human trafficking in England & Wales under the Modern Slavery Act 2015 (MSA). The key difference is that travel is required for an offence to be committed under the MSA, but this is not the case under the HTE. Evidence on the links between online platforms and child criminal exploitation are explored in a report commissioned by the Scottish Government in partnership with Children and Young People's Centre for Justice and Action for Children in 2023 - Understanding Child Criminal Exploitation in Scotland: A Scoping Review (available at: www.cycj.org.uk). This noted recruitment of young people into criminal exploitation via social media platforms, including online gaming providers. In 6D there is reference to people who 'suffer with suicidal or self-harm ideation' and further in the volume refer to people 'Suffering with their mental health'. This language can be alienating and stigmatising. Preferred language would be 'living with mental health issues' or 'people who self-harm or who have suicidal ideation'.
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]* Ofcom should consider additional guidance in this section on the gap between digital literacy and understanding of emerging risks such as AI and deepfake. Those with the poorest levels of digital literacy (for whatever reason) are most likely to be at risk.

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]* While the suggested Codes of Conduct appear appropriate, there doesn't appear to be any mechanism for external enforcement e.g. from Companies House or a Regulator. This leaves an open question as to how effective these Codes will be in practice. We would be keen to understand how these will be monitored and reviewed, and the process for that. Furthermore, any such proposals will only be as effective as the organisation overseeing them. Ofcom and the UK Government should ensure the organisation is sufficiently resourced to deliver these measures and provides regular transparent reporting on its regulatory activity and progress in relation to ensuring (as much as is feasibly possible) that providers are adhering to the Codes of Practice.
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 – but it does feel like a one size fits all proposal. Ofcom should review this approach once enacted to ensure it is effective and suitably bringing into scope all relevant services.
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? No]* There are potentially some proxy data available on implementation costs from the Data Protection Act 2018.
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	*[Is this answer confidential? No]*

Question (Volume 3)	Your response
for senior managers to positive online safety outcomes?	
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]*
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]* It would be helpful if there could be profiles by sector type to support non-commercial organisations that develop, licence or run technology platforms. Charity, community or voluntary organisations may need additional support as they are less likely to employ dedicated IT or risk professionals.
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]*
Question 10.1: Do you have any comments on our draft record keeping and review guidance?	*[Is this answer confidential? No]*

[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 3)	Your response
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]*

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]*
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]*
Question 11.3: Do you agree with our definition of large services?	*[Is this answer confidential? No]* Yes, as long as Ofcom are regularly reviewing the size and risks associated with platforms, including small, new and emerging platforms regularly.
Question 11.4: Do you agree with our definition of multi-risk services?	*[Is this answer confidential? No]* Yes, as long Ofcom are regularly reviewing the size and risks associated with platforms, including small, new and emerging platforms regularly.

Question (Volume 4)	Your response
Question 11.6: Do you have any comments on the draft Codes of Practice themselves?[2]	*[Is this answer confidential? 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]*
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]* These proposals are acceptable in principle, but Ofcom should also consider additional guidance to encourage publication of standards and performance to the public so users can have confidence and choice as to whether they wish to engage with a platform. Have Ofcom considered what, if any, support or signposting tech firms should provide to people who have a post removed when it is related to self-harm or suicide content? Although, we recognise that this content can be harmful and is removed for good reasons, this kind of content is often shared by people who are vulnerable and having their posts removed can be upsetting. How will Ofcom make sure that companies reading this Guidance are aware of appropriate signposts to seek further advice/support to share with individuals who raise concerns about content? For example, references to support, such as through the Revenge Porn Helpline.
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]*

[2] See Annexes 7 and 8.

Question (Volume 4)	Your response
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]* We agree with the proposals. Ofcom should consider potential challenges around the affordability and programming of these tools for small community/voluntary organisations.
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? No]*
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;	*[Is this answer confidential? 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
• 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.	
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]* We agree with the proposals.
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]* Ofcom should consider the development of child friendly complaints processes to empower users under 18. Complaints procedures need to be easily accessed by all users regardless of age, disability etc. and providers should be open about what action may be taken in response to complaints. We note the provision for 'trusted flaggers' to use a dedicated reporting channel for fraud due to the currently available evidence. Ofcom should regularly review the success of this approach, and consider its potential utility to report CSAM, with 'trusted flaggers' comprising Police forces, NCA, NCSC etc.

Question (Volume 4)	Your response
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]* We note that there has been some attempt to consider if policies are readable by children. However the assumption of language/style fit for legal age for use (often 14 years) is flawed. The industry is well aware that many of the most vulnerable users are under 14. Policies should be drafted for a much younger age group to protect those most at risk (accepting that users may technically be underage).
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]*
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]* The proposals are helpful. However the onus remains on the child to block/mute unwanted contact from an adult. The platform technology is sufficiently sophisticated to run searches to identify adult users who persistently make unsolicited contact with children and block them. This control needs to be strengthened and more responsibility put on operators.
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]*
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]*

Question (Volume 4)	Your response
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]*
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]*
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? No]*
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]*
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]*

Question (Volume 4)	Your response
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? No]*
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]* We are supportive of Ofcom giving further consideration to a measure recommending that users that share CSAM have their accounts blocked and consider this to be a proportionate move, given the severity of the level of harm caused by CSAM.
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?	*[Is this answer confidential? No]*

Question (Volume 4)	Your response
• How long should a user be blocked for sharing known CSAM, and should the period 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?	It is difficult to be specific but it would be helpful for Ofcom to consider a risk-based decision making framework to encourage consistency across all platforms. This would need to be considered on a case by case basis, dependent on the facts and circumstances of each case.
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]* We agree with the proposals for warnings for those seeking out CSAM online on search services. It would be interesting to consider the findings from automated tools developed by the IWF and Lucy Faithfull Foundation that pushes CSAM searchers on Pornhub to seek help for their online behaviour when these are available. In March 2022 alone, their chatbot appeared more than 170k times for those seeking CSAM on Pornhub.
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]*

Question (Volume 4)	Your response
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]*
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]*
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]* We note the recommendations outlined but also recognise that it will be for Ofcom to satisfy itself that it is exercising its duties appropriately under the relevant legislation.

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]* At 25.3 it states that Annex 5 is the Illegal Contents Judgement Guidance but understand this is an error and should be referring to Annex 10. We agree that detailed guidance is needed as providers' content moderators are being required to make really complex judgements on what constitutes illegal content. In relation to priority, relevant non-priority (other) offences, in particular at A1.30 (Annex 10), there is reference to the epilepsy trolling offence, the cyberflashing offence, the self-harm offence and the false communications offence. It

Question (Volume 5)	Your response
	should be noted that of these, only the self-harm offence has been introduced in Scotland as there is existing law in place to cover the rest. Nuances or differences in the devolved context could be more clearly teased out, as currently the jurisdictions are somewhat conflated and add to the confusion. It is not entirely clear from reading through the CSAM section which laws are relevant in which UK Nations. For example, Section A4.43 Offences related to 'paedophile manuals' and obscene articles, it is not clear from the guidance that this is not an offence in Scotland. This is a running theme throughout the sections on CSAM and grooming.
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]* This guidance is incredibly thorough, but also complicated. We think it may be difficult for services with limited access to legal expertise to confidently make judgements on what constitutes illegal content using this. We reiterate our point from Q26.1 that it is not always clear that laws may differ in Scotland from the rest of the UK.
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]*

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]* You may wish to consider listing Police Scotland [and Action Fraud] as a trusted flagger.

Question (Volume 6)	Your response
Question 29.1: Do you have any comments on our draft Online Safety Enforcement Guidance?	*[Is this answer confidential? 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 keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?	*[Is this answer confidential? No]*
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]*

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