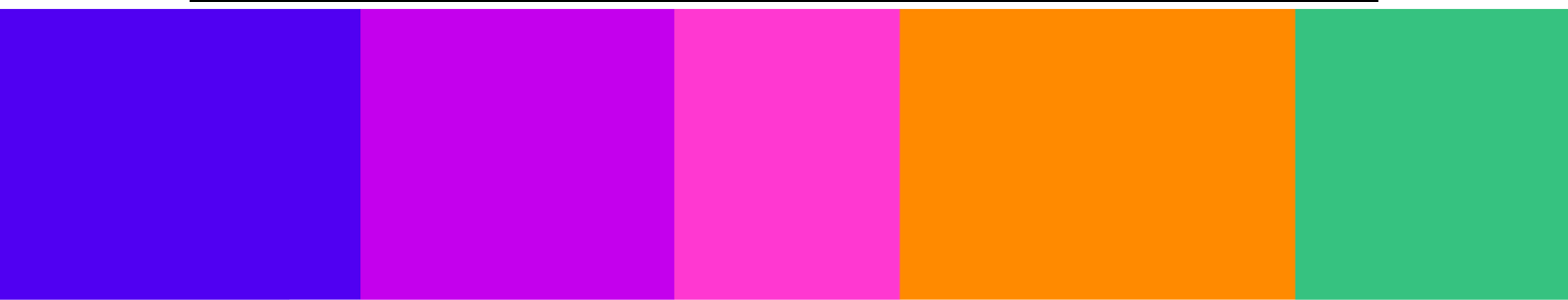


## Your response

Question (Volume 2)	Your response
<p><b>Question 6.1:</b></p> <p>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.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>The stated number of 130 offences need to be clearly listed in a easily manageable and locatable context. At present, you need to open and read several documents to find exactly what the offence is.</i></p> <p><i>References to grooming only explains the context of when it becomes illegal, however grooming itself in the initial stages is ‘legal’ chat.</i></p> <p><i>The figure surrounding URLs is incorrect as this is based on figures supplied to IWF, whereas reporting of CSAM does not fall into this currently and therefore not reported. This doesn’t account for content which is deemed as CSEM, which can be more harmful than certain cases of CSAM.</i></p>
<p><b>Question 6.2:</b></p> <p>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.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>With regards to CSEA, we are only aware of what is currently known and certain research has not been fully undertaken, or there is lack of full knowledge surrounding certain threats. ‘We’ need to have a clear and accurate picture of the CSEA past, present and future threats before ‘we’ can understanding how to fully tackle these issues.</i></p>

Question (Volume 3)	Your response
<p><b>Question 8.1:</b></p> <p>Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice? Please provide evidence to support your answer.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Most platforms (Large) have T&amp;S responsibilities outside of UK jurisdiction. How could Senior Management be held accountable if based outside UK?</i></p>



Question (Volume 3)	Your response
<p>vide underlying arguments and evidence of efficacy or risks to support your view.</p>	<p>How would any relevant and appropriate training be carried out ? who by? Each platform currently takes a different approach with no alignment or set agreed format. How could this be suitable managed. There are no formal training qualifications or courses available. 8.1 states “design &amp; operational management”, however there are 4 key areas which would require training; Product, Policy, Operations and Legal</p> <p>Who would carry our Independent Assurance checks ? How and who would be allowed to carry this out and be suitable qualified to audit? Can we rely on an ‘internal audit’ mechanism by a platform to check themselves?</p>
<p><b>Question 8.2:</b></p> <p>Do you agree with the types of services that we propose the governance and accountability measures should apply to?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>This should cover all and every “internet” enabled service including gaming, dating, shopping etc</i></p> <p>Although some will be smaller, it is imperative that all areas are covered, otherwise the gaps will encourage online harms to still occur.</p>
<p><b>Question 8.3:</b></p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>At present, to just have access to the CSEA Hash set is a paid for service, and certain criteria has to be established (rightly so) before access granted. Many companies may not have the funds available to purchase the hash data. This is before they would have to spend more money incorporating into internal systems.</i></p> <p>Again, hash data is still only what is known to Authorities, and the concern is what is ‘unknown’. There is still a lack of appropriate, relevant and effective sharing of information and intelligence across all sectors which causes confusion and delays when actioning illegal content.</p> <p>Who would be the independent third party ? This would also incur costs to train and have the relevant knowledge and expertise in each relevant online harm topic.</p>

Question (Volume 3)	Your response
<p><b>Question: 8.4:</b></p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Who would take the overall relevant responsibility when within platforms there is a struggle of power between Product, Policy, Operations and Legal teams. Who would rightly have the final say, and if there is a failure, how would this be managed.</i></p>
<p><b>Question 9.1:</b></p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>How can these Risk Assessments be undertaken solely from a UK perspective on platforms which have global reach. A harm in the UK may not be a harm in another Country, but as a platform is global, how do we assess. Anything in theory is a Risk, even something innocent – like a 'fun' challenge.</i></p> <p><i>1 of the Risk Assessments should be how it would fail regarding the OSA and impact of failure</i></p>
<p><b>Question 9.2:</b></p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Although the 4 step RA has been used in other sectors successfully, to introduce this for the online world is far more complicated. There should be further steps from educating users, re-iterating ToS, prompts, ease of reporting, action on reporting</i></p>
<p><b>Question 9.3:</b></p> <p>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?<sup>1</sup></p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>They need to be explained in a clearer way with an easier identification of all 130 potential offences. The fact the document is 1700 pages shows how complex and unclear it presently is.</i></p>

<sup>1</sup> 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
<p><b>Question 10.1:</b></p> <p>Do you have any comments on our draft record keeping and review guidance?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Draft record keeping should be in a set agreed format across all platforms. If each platform utilises a different approach this will cause mis alignment and terminology will be viewed differently.</i></p>
<p><b>Question 10.2:</b></p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>It has to be all follow the same rules or they don't. If OFCOM exempt certain services, this will be seen as direct action against particular services, rather than a whole approach to online safety.</i></p>

Question (Volume 4)	Your response
<p><b>Question 11.1:</b></p> <p>Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>A phrase is stated "existing good practice"- however if there was currently good practice, there wouldn't be so many illegal harms. Who has deemed a practice 'good' and how was this identified ?</i></p>
<p><b>Question 11.2:</b></p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>No, this should be fully across the whole spectrum of platforms and sites.</i></p>

Question (Volume 4)	Your response
<p><b>Question 11.3:</b></p> <p>Do you agree with our definition of large services?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>As a definition this would be acceptable, however, many illegal harms happen across a multitude of small to large platforms, so this would mean users may move from a large to a small platform, which could then in turn become larger user base.</i></p>
<p><b>Question 11.4:</b></p> <p>Do you agree with our definition of multi-risk services?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>No, an illegal harm should be viewed as it is, whether in conjunction with other harms or not. Any platforms can have various risks associated for all sorts of reasons, even those that may seem ‘innocent’.</i></p>
<p><b>Question 11.6:</b></p> <p>Do you have any comments on the draft Codes of Practice themselves?<sup>2</sup></p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>As this is a highly complex and new set of codes, it should be clearer and easier to search the codes and see how they all interact with the OSA.</i></p>
<p><b>Question 11.7:</b></p> <p>Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>With regards to CSAM hash costs, some of these figures appear incorrect (taken from personal experience), and also do not appear to show ‘membership’ fees to organisations that can supply the hash data. It also refers to ‘known’ CSAM, however, we also need to know about ‘unknown’ and ‘new’ CSAM. The other factor to consider is the detection of CSEM, which is not currently hashed, but can be more harmful and illegal than certain CSAM.</i></p> <p><i>The figures for actionable content from NCMEC referrals isn’t clear to make a full judgement of costs about safeguarding.</i></p> <p><i>The figures shown are from 2022, we are now at the end of 2023, so any figures obtained are out of date</i></p>

---

<sup>2</sup> See Annexes 7 and 8.

Question (Volume 4)	Your response
<p><b>Question 12.1:</b></p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>'Performance Targets' is a bad idea for content moderators! These people are already under huge pressure with regards to timescales and content view. To add a 'target' will enhance this pressure and could lead to damaging welfare and mental health implications. To suggest 'Performance Targets' shows a clear lack of knowledge around this type of work!</i></p> <p><i>There should be a focus on training, rather than targets.</i></p> <p><i>Policies and Processes are already in place in many platforms, and is clearly not as effective as it should and could be. There is no alignment or coordination around content moderation, which is the key area to be addressed.</i></p>
<p><b>Question 13.1:</b></p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>'Performance Targets' is a bad idea for content moderators! These people are already under huge pressure with regards to timescales and content view. To add a 'target' will enhance this pressure and could lead to damaging welfare and mental health implications. To suggest 'Performance Targets' shows a clear lack of knowledge around this type of work!</i></p> <p><i>There should be a focus on training, rather than targets.</i></p> <p><i>If content is illegal – why would it be downranked. IF illegal, it should be removed and reported.</i></p> <p><i>How can a platform distinguish between legal/illegal when a search could be global.</i></p> <p><i>If a user searches for 'anime japan' – legal</i></p> <p><i>But some results could be illegal for UK</i></p>

Question (Volume 4)	Your response
<p><b>Question 14.1:</b></p> <p>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.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>To tackle the illegal harm of online-CSEA, we need to take into account CSEM as well as CSAM. There is as much harmful illegal CSEM content as there is CSAM. Hash matching only works on 'known' content, not 'unknown'. There is a huge gap in how quickly an image can be hashed and shared around LEAs and platforms, therefore on 1 platform it could be hashed, and another it isn't and still in circulation.</i></p> <p><i>To purchase this service is not only an added cost to a platform, but also the tech installation. How can they keep updated as much as possible with all the new hash matches, how quickly does it take.</i></p> <p><i>Which Hash dataset is the best, who decides ? There are several hash sets (PDNA, MD5, Shah) – so does a platform require all 3 ?</i></p> <p><i>CSAM URL detection only works if the URL has been confirmed as CSAM (or infact CSEM). To check each URL is time consuming for platforms, LEAs and other Agencies. The option here is to review and assess other context of the image/post/comment. Offenders will and do know about detection capabilities, so will edit, change and alter URLs with other characters to disguise the URL – this would again add further costs and resources to identification.</i></p>
<p><b>Question 14.2:</b></p> <p>Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>No</i></p>
<p><b>Question 14.3:</b></p> <p>Do you have any relevant evidence on:</p> <ul style="list-style-type: none"> <li>The accuracy of perceptual hash matching and the costs</li> </ul>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>As mentioned above, the issue with Hash matching is 'known' v 'unknown', and now also to include content that doesn't or wouldn't fall under hash matching, ie. CSEM content and also AI Gen CSEA content. The figures provided don't represent a true representation of reported content,</i></p>

Question (Volume 4)	Your response
<p>of applying CSAM hash matching to smaller services;</p> <ul style="list-style-type: none"> <li>• 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;</li> <li>• The costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching<sup>3</sup> for CSAM URL detection;</li> <li>• The costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services; and</li> <li>• 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.</li> </ul>	<p><i>as reports can be received from multiple sources, not just NCMEC. The key point is prioritising CSAM. Cat A would be the highest and the key focus area. If we follow the path from what is reported to NCEMC – to UK NCA – then to Regional Police Forces – then Investigation. What is the actual % of these reports being investigation further and then leading to successful outcome.</i></p> <p><i>The cost of applying such measures, as well as training to smaller services isn't viable, but to enhance knowledge and training to these companies is a cheaper and easier option.</i></p> <p><i>However, maybe consideration should be given to supply the hash data for free ? Potentially funded by Government ?</i></p> <p><i>We need to consider how often this data would be updated and how quickly. If its every 6months, then that's a huge amount of new data, and a lot in circulation during the 6months.</i></p> <p><i>Hash data is only a single part of CSEA detection, as mentioned there are URLs, keywords and other indicators. A more centralised, information sharing approach would be more advantageous and work out cheaper and resource effective for smaller companies.</i></p>

<sup>3</sup> 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
<p><b>Question 15.1:</b></p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>The proposals in theory are good, the reality is different. How many sources would be supplying identified URLs, how quickly, how time intensive will it be keeping it updated. Who is checking the URLs, who are the experts supplying the lists ? Unless there is a coordinated approach, then this is an impossible request for companies to achieve</i></p>
<p><b>Question 16.1:</b></p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>There needs to be consistency and ease of reporting and making complaints. Users want a response in a timely manner and what happens if they disagree with a decision. Who and how can they respond to then? Complaining is a timely process. If a platform doesn't overturn an action and a User requires a super complaint, how long will this process take.</i></p>
<p><b>Question 17.1:</b></p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Most platforms have ToS policies easily available, and they do state what is allowed on the platform. However, users still post, share and distribute illegal content. Certain platforms now have a block if you type in certain banned words, this is a good example that could be followed by others.</i></p>
<p><b>Question 17.2:</b></p> <p>Do you have any evidence, in particular on the use of prompts, to guide further work in this area?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>As above, the banning of keywords is a good start. Platforms should have direct links to policies from their 'home' pages.</i></p>
<p><b>Question 18.1:</b></p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>This is an umbrella approach with regards to those under 18. It would be advantageous to take on research with regards to under 18yr users, as it is evidences that those aged 15-17 dislike being seen or treated as children, and</i></p>

Question (Volume 4)	Your response
	<p><i>will therefore find ways around any age verification/assurance. There is a need to understand how these young people use certain social media – for those in a school environment these actions could and would be detrimental, and potentially push young users onto other platforms that aren't following OFCOM regulations. OFCOM need to also understand the pre nature of grooming, which is usually 'legally' allowed chat.</i></p>
<p><b>Question 18.2:</b> Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Unfortunately all you have to do is go on a search engine and it explains how to change settings, so young people would most probably do this.</i></p>
<p><b>Question 18.3:</b> Are there other points within the user journey where under 18s should be informed of the risk of illegal content?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>U18s are more than likely already aware of what is illegal content, and in many cases are intent in finding it (example: vapes, drugs). It should be clearer about what action will be taken or a warning notice as a pop up if a user under 18yrs searches/requests etc illegal content.</i></p>
<p><b>Question 19.1:</b> Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Yes. However, all platforms would have to share relevant information and agree on content to be removed or blocked. If 1 platform allows 1 type of content, but another disallows, then the content can still be available.</i></p>
<p><b>Question 19.2:</b> What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Relevant and appropriate training by approved professionals would be suitable for smaller companies, with an audit check of compliance</i></p>

Question (Volume 4)	Your response
<p><b>Question 19.3:</b></p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>IP blocking – if a user has violated a policy/policies, it is possible to block the IP from accessing the platform.</i></p> <p><i>The same can be utilised for contact details (e-mail, phone numbers)</i></p> <p><i>There are chat bots which can pop up if a user is searching for illegal content and advise them accordingly.</i></p> <p><i>Blurring technology can be utilised for 18+ content until a user confirms their age.</i></p> <p><i>Information sharing across platforms regarding the most up to date illegal harms, trends and patterns can help change how design parameters are introduced.</i></p>
<p><b>Question 20.1:</b></p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Blocking offending users is a good initial safety feature, however, it is known that some offending users will just set up new accounts and continue the ‘abuse’ in whatever form. It will also depend on the type of harm being caused and the reason why it is happening. Need to consider how to stop unwanted attention after initial blocking has been activated.</i></p>
<p><b>Question 20.2:</b></p> <p>Do you think the first two proposed measures should include requirements for how these controls are made known to users?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>In theory yes, but there are already instructions in Safety help centres how to activate ‘blocking’ and options are already. Suggest ‘block’ options should be clearer and more obvious</i></p>
<p><b>Question 20.3:</b></p> <p>Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>This has been proven to have an element of risk, as some users will attempt to become ‘verified’ to avoid certain repercussions. Also, certain platforms will not take action on verified accounts even though they might be ‘offending’ in some way.</i></p>

Question (Volume 4)	Your response
<p><b>Question 21.1:</b></p> <p>Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p>
<p><b>Question 21.2:</b></p> <p>Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically:</p> <ul style="list-style-type: none"> <li>• 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?</li> <li>• How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed?</li> <li>• 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</li> </ul>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>It is highly possible to block a user using various options such as IP, phone number, e-mail, and on some platforms this is already undertaken, but not on large scale enforcement. It is also possible to identify patterns of re-occurring offenders using different style of user names. Consideration also needs to be given to pushing offenders onto other platforms – could certain information be shared across platforms? If offending users are only be looked at for the most serious harms, then any impact should be seen as positive</i></p> <p><i>This is a valuable recommendation, and 1 with serious merit. I'd highly suggest there should be an option for a time length of a block depending on the circumstances.</i></p> <p><i>This contradicts points made earlier with regards to Hash data and it's accuracy. If, as OFCOM state, hash data is accurate, then no content should be erroneously identified. The specific point is what is being classed as CSAM, as in some cases, legal content can be deemed as CSAM (anime, innocent family images). Certain platforms already remove content that might be deemed CSEM, but leave the account 'open', this is 1 possible solution. Warning notes are also passed to user requesting removal of content, and if they don't oblige, then a block is added until they do. The other consideration is how to stop users just setting up</i></p>

Question (Volume 4)	Your response
<p>risks and impacts on user rights?</p>	<p><i>new accounts if they have been blocked. This is sometimes easier than waiting for an appeal against a violation or if they have been suspended.</i></p>
<p><b>Question 22.1:</b> Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Yes, and some platforms already utilise such tooling. However, it has to be carefully considered what type of words would and could be deemed as harmful or those used to search for CSAM content. Clarification needs to be sought if only for CSAM or CSEA related content. Once Users realise certain wording is 'flagged', they will use different methods, so it would be imperative to keep this information shared and updated.</i></p>
<p><b>Question 23.1:</b> Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Costs for low risk small and micro business can be adapted by different approaches than those stated. For instance, improved training for staff on certain topics, simple and easy reporting and better understanding of the OSA and Ofcom reg's. These would be cheaper alternatives for certain businesses.</i></p>
<p><b>Question 23.2:</b> 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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>As above, with enhanced training and knowledge, which could be cheaper and more effective, any business that is at significant risk could minimise any potential risks occurring. This could also include a pre audit check to allow them to review current measures and improve, with a re-audit within a year before Ofcom take any further action.</i></p>
<p><b>Question 23.3:</b> We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Yes, however, although large services have more users and more financial backing, this does also come with more complex handling of these issues. Due to the amount of users and content, and even with use of technology, it can be</i></p>

Question (Volume 4)	Your response
	<p><i>more challenging. Have access to resources to 1 thing, have access to the right resources and information is another.</i></p>
<p><b>Question 24.1:</b> 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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p>Yes</p>

Question (Volume 5)	Your response
<p><b>Question 26.1:</b> Do you agree with our proposals, including the detail of the drafting? What are the underlying arguments and evidence that inform your view.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Clarity needs to be issued with exactly what is deemed 'illegal'. Certain CSAM content will be illegal in UK, but not in other Countries – how will services handle that? Initial forms of grooming is NOT illegal, but concerning behaviour, further clarification required.</i></p> <p><i>What, or how and who will consider a threat, abuse or harassment. It's possible to view content that maybe deemed 1 of these, but it can also be view as 'banter', especially when no context is applied. 1 users view could be very different to another users.</i></p> <p><i>Clarification also required regarding what is 'obscene' – individuals have different perspectives, views and interests and this could be against freedom of expression of what a individual likes.</i></p>
<p><b>Question 26.2:</b> Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Although the guidance is accessible, it's not set out in a clear manner and not detailed enough. It would be advantageous to be able to search or find relevant points (drop down menu?) in the style of a quick guide. At present it adds more confusion to understanding the process and guidance. There</i></p>

Question (Volume 5)	Your response
	<p><i>is no further guidance, and already services are finding it confusing and complicated, therefore it must be clearer to understand.</i></p>
<p><b>Question 26.3:</b></p> <p>What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>The topics covered are reasonable to an extent of what could or would be deemed illegal from an over arching perspective, however, the reality of working in this environment is very different as context in a lot of these topics is highly relevant. For platforms to action (report) all content under the ICIG would and could over burden systems and agencies.</i></p>

Question (Volume 6)	Your response
<p><b>Question 28.1:</b></p> <p>Do you have any comments on our proposed approach to information gathering powers under the Act?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>No comments at present</i></p>
<p><b>Question 29.1:</b></p> <p>Do you have any comments on our draft Online Safety Enforcement Guidance?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>6 months to be compliant with the act does seem quite short timescale for some services. To include identifying new potential systems, testing, training etc and certain costs, this should be extended to 1 year.</i></p> <p><i>What action will be taken if services don't comply? It could be cheaper to be fined than implement all new and necessary requirements.</i></p> <p><i>There is still the requirement to clarify illegal content</i></p>

Question (Annex 13)	Your response
<p><b>Question A13.1:</b></p> <p>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?</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>Agree to positive effect</i></p>
<p><b>Question A13.2:</b></p> <p>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.</p>	<p><i>[Is this answer confidential? Yes / No (delete as appropriate)]</i></p> <p><i>N/A</i></p>

Please complete this form in full and return to [IHconsultation@ofcom.org.uk](mailto:IHconsultation@ofcom.org.uk).