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]* Under Article 10 of the European Convention on Human Rights (hereinafter, ECHR), everyone has the right to freedom of expression, which encompasses the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. These freedoms may only be legitimately restricted upon fulfilling the three-prong test: legality, necessity and proportionality. Restrictions need to be prescribed by law and necessary in a democratic society. They must also be proportionate and pursuant to legitimate aims and purposes. Under Article 1 of the European Convention, states have the duty to respect and to guarantee the rights therein recognized to everyone under their jurisdiction. Article 19 of the International Covenant on Civil and Political Rights (hereinafter, ICCPR) provides similar protections. International human rights law and European human rights law require that states differentiate between illegal and permissible content. Per the legality requirement, restricted speech needs to be clearly and unambiguously identified in a law. Therefore, we are worried that section 10(2)(c) puts on companies the burden of taking action to mitigate "the risks of harm to individuals", without specifying that such a harm must derive from an illegality. This open-ended wording, coupled with those of sections (9)(5)(f) and (g), is a breach of the legality principle and allows for discretionary interpretation by the enforcement authorities. In addition, by making harm autonomous from the illegality of content and signaling legal expression as the causes of harm that must be dealt with, it creates incentives for companies to remove all kinds of "legal but harmful" content. Any government mandate requiring or

Question (Volume 2)	Your response
	setting incentives for companies to take action vis a vis these kinds of content is contrary to Human Rights Law. Moreover, the inclusion in the Act and in the implementing guidelines of some categories of lawful content within the "online harm" category, such as offensive content and disinformation ("false communications offense", section 179 of the OSA and section 6Q of "Volume 2: The causes and impacts of online harm" in this consultation) is particularly worrysome. Not only is the offense of "false communications" an overbroad, disproportionate restriction to freedom of expression, but it is also easy to weaponize against political dissidents or people holding diverging views on societal issues. Moreover, sections 180 and 181 of the OSA and paragraph 6Q.4 of Volume 2 of the consultation do not exclude those persons who forward or share the message without the intent of causing harm.
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]* As OFCOM acknowledges, encryption and pseudonimity are important aspects of the protection of the right to privacy, enshrined in article 8 of the ECHR and article 17 of the ICCPR, which the UK has a duty to secure (ECHR, art. 1). Under international Human Rights Law, states cannot interfere with privacy unless by law and if necessary in a democratic society. Private, secure communications are essential to freedom of expression. When communications are not private, people tend to self-censor themselves. The mediate effects of this situation are even worse. Since the internet is the place where a large part of public debate takes place, an effect of self-censorship of the mentioned characteristics will discourage deliberation and citizen involvement in common matters. The right to obtain information about public interest issues will be infringed upon, thus seriously affecting the breadth and robustness necessary in the public debate of a democratic society. It is problematic, then, that OFCOM refers to end-to-end encryption, pseudonimity and anonymity and livestreaming as "posing particular risks'' that should be dealt with. If anything, they are the centerpiece of internet privacy. What is more, they are essential tools for

Question (Volume 2)	Your response
	journalists and human rights defenders to carry out their essential jobs. Finally, if anonymity or encryption were curtailed in any way, the negative effect on freedom of expression would have a disparate impact on vulnerable populations, political dissidents, and ethnic, religious and gender minorities. As for livestream services, also signaled as a risk, it must be taken that they can provide invaluable information in the access of all persons to information, as they have proven to be essential in the diffusion and/or coverage of social protests and other events of political and social relevance. While we applaud OFCOM's efforts to curb the circulation of CSAM images and incitation to terrorism, we believe they should be conducted in strict compliance to international human rights law, especially the right to privacy and freedom of expression. Consequently, no measures should be taken that entail hampering encrypted communications in any way, such as requiring providers of such services to scan those communications in search of infringing materials, per section 121(2)(a).

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]* As for rule 3A in connection with risk assessments (see page 11 and page 10), in line with our previous replies, we suggest the enforcement of the "risk-centered" approach to platform governance takes Human Rights Law, and specially freedom of expression, seriously. Therefore, the enforcement efforts must make sure that risk mitigation measures of harmful content by platforms are legal, necessary and proportionate.

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]* *While size and risk are generally good indicators, the types of duties could be tailored to the capacity of companies to comply with them. For instance, it should be taken into account whether a company provider of a smaller service is a startup or is part of a bigger holding that counts with the financial resources to comply with assessment and mitigation duties. Conversely, a large service is provided by a company that is, for some reason, unable to comply with all duties imposed to those services, such as the case of nonprofits (i.e. Wikimedia)*
Question 8.3: Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?	*[Is this answer confidential? No]* Article 37 of the Digital Services Act of the European Union (DSA) requires Very Large Online Platforms and Very Large Search Engines (VLOPs and VLOSEs) to undergo independent audits at least once a year, to assess their compliance with due diligence obligations, commitments arising from codes of conduct and crisis protocols. Organizations carrying out the audits must comply with the following requirements: independence; expertise in the area of risk management, technical competence and capabilities; and objectivity and professional ethics. In case OFCOM were to adopt provisions requiring third-party auditing of measures to mitigate and manage illegal content risks, the requirements set out in the DSA should be adopted. In addition to the aforementioned requirements, the entity performing the audit should have proven expertise or hire a group of professionals with proven expertise in the area of human rights impact assessments. Moreover, OFCOM could provide guidance to the companies carrying out the audits to ensure that the methodology followed is uniform and complies with the Act's goals.
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]* The idea of tying remuneration for senior managers to positive online safety outcomes lies on the assumption that it could incentivize them to achieve better results. We believe this is not a safe assumption and we agree with

Question (Volume 3)	Your response
for senior managers to positive online safety outcomes?	OFCOM's decision not to propose a measure regarding remuneration in this version of the Code of Practice. If anything, senior managers will be encouraged to over remove/deindex/downrank borderline and permitted content, since the only metric that will be utilized to measure the effectiveness of their job will be "safety" (i.e. the absence of illegal and/or "harmful" content). Under such a scheme, there is a risk that other principles, such as freedom of expression and other human rights, are sacrificed for the sake of a "safer" environment. This could have pernicious effects on the openness of public debate, diversity and pluralism online. Alternatively, if satisfactory results (from a "safety" standpoint) were not achieved, a system tying remuneration to results could lead managers to misrepresent their achievements, which would distort the general picture of the situation of online safety. This, in turn, can mislead authorities into making policy decisions based on inaccurate reporting by the regulated companies.
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]* *This question is addressed to regulated services*
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]* *This question is addressed to regulated services*

Question (Volume 3)	Your response
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]* *This question is addressed to regulated services*
Question 10.1: Do you have any comments on our draft record keeping and review guidance?	*[Is this answer confidential? No]* Documents resulting from record keeping and review obligations should be public. OFCOM should make these documents publicly available in an easily accessible database. OFCOM should afford companies the chance to request, under well-founded reasons, that certain documents be either wholly or partially exempt from public release.
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? Yes / No (delete as appropriate)]* Yes

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]* *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 4)	Your response
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]* *Yes. We believe the size of the services is one among many factors that can make a service more risky than others. That is why we find positive that the risk is defined using size among other factors and a risk matrix. It could be the case that the size of the service, measured by its user base, is not a good indicator of its ability/resources to comply with these measures or the risks it entails, as could be the case of Wikipedia. Some more tailored mechanisms could be used in order not to drive not-for-profit platforms out of business.*
Question 11.3: Do you agree with our definition of large services?	*[Is this answer confidential? No]* *Yes. A service is deemed as large when it has an average user base greater than 7 million per month in the UK, approximately equivalent to 10% of the UK population.*
Question 11.4: Do you agree with our definition of multi-risk services?	*[Is this answer confidential? No]* *Yes. A service is deemed as multi-risk where it is assessed as being medium or high risk for at least two different 2 kinds of harms from the 15 kinds of priority illegal harms set out in the Risk Assessment Guidance.*
Question 11.6: Do you have any comments on the draft Codes of Practice themselves?[2]	*[Is this answer confidential? No]* *We applaud that the codes of practice explicitly state that Ofcom must carry out its functions compatibly with the Human Rights Act 1998, including the rights to freedom of expression and privacy.* *However, we believe the guidance set out in sections 4A of in Annex 7 and Annex 8 respectively, which requires providers to have systems or processes designed to delete (for u2u services) or deindex or downrank (for search engines) illegal content of which it is aware poses risks to freedom of expression. We believe that companies should not be entrusted with the task of making "an illegal content judgement in relation to the search content" and to take action in connection with that content if they believe it is illegal. Except for the case of CSAM images,*

[2] See Annexes 7 and 8.

Question (Volume 4)	Your response
	*where a hash matching system could work to make these determinations in an automated manner, decisions on the illegality of contents should be made by judiciary authorities and not outsourced to platforms, which are ill-fitted to make them and will be incentivized to err on the side of caution and over-*remove/deindex/downrank *borderline content.* *Performance targets set out in section 4C rely on the prerogative of platforms to make determinations on the illegality of contents, that should only be retained for CSAM content through automated hash systems. Other than that, platforms should not be making determinations on the illegality of the content and therefore we believe the time in which illegal content remains online is not a good metric, for it could create incentives for a rapid* removal/de-indexing/downranking *of any content deemed suspicious.* *As for section 4F, we believe specific training should be administered to human moderators and policy officers in international human rights, especially in freedom of expression and privacy.*
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*
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]* *See answer to question 11.6*

Question (Volume 4)	Your response
Question 13.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]* *See answer to question 11.6*
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 proposal for CSAM hash matching and CSAM URL detection. As for fraud keyword detection, we believe automated systems could be used as long as platforms provide safeguards against removal of legal content, such as the intervention of human moderators to confirm the accuracy of machine-made decisions.*
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]* *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;	*[Is this answer confidential? No]* No

Question (Volume 4)	Your response
• 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.	
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]* *Yes*
Question 16.1: Do you agree with our proposals? Please provide the underlying	*[Is this answer confidential? Yes / No (delete as appropriate)]* *As for Volume 16, we agree that services ought to put in place an easy to use complaint procedure. As for the creation of a dedicated channel for trusted flaggers, we*

[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
arguments and evidence that support your views.	*believe that state actors with relevant expertise would be helpful in signaling possible fraud.*
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*
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? Yes]* *Yes*
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? Yes / No (delete as appropriate)]* *The language informing the children the measures they can take and the consequences of their actions online could be tailored to meet the needs of different age groups.*
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? Yes / No (delete as appropriate)]*

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? Yes / No (delete as appropriate)]*
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? Yes / No (delete as appropriate)]*
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 / No (delete as appropriate)]*
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]* *We agree that blocking other users empowers users to decide who can see their activity online and interact with them. However, allowing government accounts and public officers' personal accounts to block the account of citizens could pose difficulties in the citizens' of access to*

Question (Volume 4)	Your response
	information if that block entails that the person will be unable to access the content posted by the office/officer in question.
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]* *The verification system should be as transparent as possible and end users should have instant access to the reasons why a certain account is verified. It is also advisable that if any sign or badge is used to show "verified status", it is different from any other badge conferred to users that hold a "premium" membership given by a paid subscription.*
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 / No (delete as appropriate)]*
Question 21.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]* *No*
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	*[Is this answer confidential? Yes / No (delete as appropriate)]* No

Question (Volume 4)	Your response
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 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 (delete as appropriate)]* *Yes*

Question (Volume 4)	Your response
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? Yes / No (delete as appropriate)]*
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? Yes / No (delete as appropriate)]*
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? Yes / No (delete as appropriate)]*
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? Yes / No (delete as appropriate)]*

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]* *We believe that companies should not be entrusted with the task of making an illegal content judgement in relation to the search content and to take action in connection with that content if they believe it is illegal* *Except for the case of CSAM images, where a hash matching system could work to make these determinations in an automated manner, decisions on the illegality of contents should be made by judiciary authorities and not outsourced to platforms, which are ill-fitted to make them and will be incentivized to err on the side of caution and over-*remove/deindex/downrank *borderline content.*
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]* *See answer to question 26.1*
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]* *See answer to question 26.1*

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]* *No*

Question (Volume 6)	Your response
Question 29.1: Do you have any comments on our draft Online Safety Enforcement Guidance?	*[Is this answer confidential? Yes / No (delete as appropriate)]* *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? Yes / No (delete as appropriate)]*
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? Yes / No (delete as appropriate)]*

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