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? Yes / No (delete as appropriate)]* Overall, we are satisfied with the causes and impacts of online harms as detailed in Volume 2 of the consultation. Online hate is even more specific to the Jewish community, as both a religious and racial/ethnic group (although presently lacking that legal distinction in the UK). Antisemitism, particularly over the last ten years, has become a far more accepted norm in the UK, particularly through the use of social media. It is also a matter of hate begetting hate, people likely feel more comfortable 'retweeting' or sharing antisemitic content when it has been posted by another person. *We would also query the statistics given in the companion document regarding the percentage of users that have encountered 'hateful, offensive or discriminatory content' online, particularly as this refers to 11% of all internet users and 16% of minority ethnic. The percentage of Jewish Internet users encountering online hate is far higher than this, which makes us wary of the statistics stated above[1].*
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? Yes / No (delete as appropriate)]* We agree that religion, race and ethnicity are strong factors in online illegal harms that can be affected by those listed in the consultation. Antisemitism is particularly prevalent on social media and we have seen instances where people engaging in antisemitic activity have been arrested and found guilty of their conduct on video sharing platforms. However, we have also seen a significant number of UK users engaging in antisemitic hate speech online who have faced no repercussions either from social media platforms or the law.

[1] Twitter: The Extent and nature of antisemitism on Twitter in the UK

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? Yes / No (delete as appropriate)]* We think they can be stronger. While it would be a great improvement which would hold services to account for allowing various forms of illegal harms to take place on their platforms, there need to be more consequences for those who breach such Codes. This mechanism is heavily reliant on not only the dedication and hard work of employees, but also a thorough understanding of the harms. Antisemitism is often referred to as "the oldest hatred" - it has evolved, adapted and expanded over time. There are nuances that people do not understand; to an uneducated onlooker a picture or a statement might seem perfectly benign, but to many Jews it would not be seen as such. An example was the defence by Jeremy Corbyn of a mural called "Freedom for Humanity", which featured wealthy men, caricaturised with stereotypical depictions of Jews, playing a board game balanced on the bent backs of the suffering masses. For the mechanisms suggested to work effectively, thorough training on various forms of online harms, including antisemitism must be given by respected providers for the teams and individuals involved by the relevant group. This scheme, when it comes to religious, ethnic and racial hatred is also heavily reliant on ensuring that the individual has no bias towards all relevant groups. We have seen instances where organisational 'Heads of Diversity' have spouted antisemitic hatred, and one instance where a member of Ofcom's Online Harms team expressed sentiments with regard to Israel which were clearlu unacceptable. We would also like to see assurance that codes of conduct will lead to bans on users who espouse antisemitic views on services within the scope of these codes. We also be-

Question (Volume 3)	Your response
	lieve that mechanisms should be put in place to investigate any anonymous or dummy accounts that may be used by previously banned users. There needs to be a focus on users as well as service providers.
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? Yes / No (delete as appropriate)]* The measures should also be universal, it is worrying that smaller organisations do not have certain requirements placed on them when they are often most guilty of fostering illegal harms. There is no reason as to why smaller service providers should not be subject to staff training for content moderation to enable them to take down illegal harms. Not training staff could have the opposite effect that the Online Safety Bill aims to achieve as it would portray a perceived acceptance that the service in question may be used to espouse antisemitic and other racial hatreds. As we mentioned in a previous answer, antisemitism can be complicated to fully understand. Many people do not understand it and its monitoring requires comprehensive training to identify certain phrases and statements. Smaller services should also enable their users to block others who are targeting them or using offensive language and prevent some from commenting on their posts. Not making these rules universal across all services will merely enable them to become hubs of illegal harms.
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	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 3)	Your response
have measures to mitigate and manage illegal content risks audited by an independent third-party?	
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? Yes / No (delete as appropriate)]*
Question 9.1: 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 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? Yes / No (delete as appropriate)]* The four-steps are, *prima facia,* strong and set out a good mechanism for the process in which an online harm could be assessed and dealt with. However, there should be a fifth step, centred on sanctions. Either for the service that fails to adequately address the harm to the damaged party's satisfaction, or to the guilty party themselves. There is a huge risk here that services will not wish to adequately punish bad users and Ofcom needs to instil themselves with the power to penalise either the service or the bad actor themselves. 'Naming and shaming' is not enough. It must be in Ofcom's policies and remit to actually sanction bad users.

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?[2]	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 10.1: Do you have any comments on our draft record keeping and review guidance?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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, all services should be subject to the same record keeping rules.

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? Yes / No (delete as appropriate)]*

[2] 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? Yes / No (delete as appropriate)]* As stated above, they should be universal.
Question 11.3: Do you agree with our definition of large services?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 11.4: Do you agree with our definition of multi-risk services?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 11.6: Do you have any comments on the draft Codes of Practice themselves?[3]	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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? Yes / No (delete as appropriate)]*

[3] 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? Yes / No (delete as appropriate)]*
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)]*
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? Yes / No (delete as appropriate)]*
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? Yes / No (delete as appropriate)]*
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	*[Is this answer confidential? Yes / No (delete as appropriate)]*

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

[4] 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 16.1: 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 17.1: 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 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? Yes / No (delete as appropriate)]*
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 / No (delete as appropriate)]*
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)]*
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? Yes / No (delete as appropriate)]*

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? Yes / No (delete as appropriate)]*
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)]*
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? Yes / No (delete as appropriate)]*

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?	
Question 22.1: 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 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	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 4)	Your response
for whom we propose to recommend more measures?	
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? Yes / No (delete as appropriate)]* Overall we are happy with the drafting of volume 5. We particularly agree with the notion that sharing or forwarding a previously shared post for the purposes of expressing support or bringing what may be perceived to be positive attention to the views expressed should be considered a distinct act of an online harm in and of itself. In the case of bots, the original poster should still be considered as have committed an online harm. However, we are concerned with the language in paras 26.63, 26.64, and 26.90 to 26.114 as it appears to give 'a free pass' to those sharing content that purport to support terrorist groups. A significant number of proscribed terror groups in

Question (Volume 5)	Your response
	the UK are antisemitic and call for the annihilation of the Jewish State and world Jewry. We have seen instances of individuals in the UK adding an inverted red triangle to their X handles showing an affinity for Hamas. These posts have been shared widely and defend a proscribed terror group in the UK. The Terrorism Act's restrictions on showing support for a proscribed group must be considered in the scope of the guidance otherwise it nullifies aspects of the law which must be upheld. The onus is on the bad actor to prove that they were unaware of the content they were sharing when investigates, not on the service provider or a small number of employees to determine this. It is not enough to state that organisations should only act 'if they are aware' of signs and logos of support for proscribed terror groups. Ofcom should become aware and notify services of what it is their duty to monitor. Private groups, if it is known that this is where this content is more likely to be shared, should be required to allow access to an external moderator that can identify these signs.
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? Yes / No (delete as appropriate)]* There should be a clear cut breakdown for the offence and guidance on how to address it in the form of a table or basic breakdown. Aspects of the consultation are vague and unclear, as with the paragraphs on terrorism referenced above. Some of the language appears to give services 'an out' of not addressing online harms if they merely claim to not have the capacity to understand what is being said online.
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? Yes / No (delete as appropriate)]* The information should be maintained, updated and provided by Ofcom, or specialist groups and be handed to Ofcom to share with services. Ofcom has the responsibility as the regulator to ensure that services are aware of the dangers online and will be unable to regulate if different services have different understandings of the issues at hand. Ofcom's power will

Question (Volume 5)	Your response
	be curbed through services’ lack of understanding. Not knowing the law is not an excuse for breaking it.

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? Yes / No (delete as appropriate)]* These are acceptable and appear to allow Ofcom to effectively investigate breaches of the rules.
Question 29.1: Do you have any comments on our draft Online Safety Enforcement Guidance?	*[Is this answer confidential? Yes / No (delete as appropriate)]* We agree that the financial penalty powers set put in Volume 6 are strong and act as a reasonable punishment for services that breach rules or fail to comply with an investigation. We similarly find the Business Disruption Measures acceptable; however, for the most egregious offenders or those whose base is predominantly used to foster Online Harms, a total shutdown should be included as a penalty.

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	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Annex 13)	Your response
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? Yes / No (delete as appropriate)]*

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