Your response

Question	Your response
Question 1: Do you agree with our proposed guidance on scope? If not, please provide any information or evidence in support of your views, including descriptions of services or content where you consider it is unclear whether they fall within the scope of Part 5.	Confidential? – Y / N
Question 2: Do you have any comments on how our proposed guidance applies in respect of pornographic content created by generative-AI services within the scope of Part 5? Please provide any information or evidence in support of your views.	Confidential? – Y / N

Question 3: Do you have any comments on our proposed guidance in respect of the kinds of age assurance which could be highly effective? If you consider there are other kinds of age assurance which have not been listed that you consider could fulfil the proposed criteria, please identify these with any supporting information or evidence.	Confidential? – Y / N There is currently little evidence that an at-scale deployment of age verification/assurance which does not include the banking system can be successful. This covers the vast amount of content online and much of what could considered sexual or pornographic. It is nearly impossible to benchmark what could be considered highly effective. At the same aiming for an unquantifiable measure introduces significant privacy risks, threats to freedom of expression, places many adult users at risk of blackmail and even creates personal safety threats as identities and locations could be revealed. While there have been some claims that age verification by websites could be conducted in a fully secure manner, the reality is that cases of identity theft, fraud, and the many examples of data leaks and servers being compromised, show online data remains vulnerable. It is also at risk from hackers who are already inside a system. IBM's estimates place the average time it takes a company to detect a breach at around 200 days. This provides ample time for hackers to set up a 'man in the middle' attack to capture people's data as it is provided. In Australia, the federal government has announced it will not force adult websites to use age verification due to concerns about privacy and the 'lack of maturity' of the technology. With their government stating on record that 'at present, each type of age verification or age assurance technology comes with its own privacy, security, effectiveness or implementation issues.' As the British Computer Society (BCS) argued, regulation should "not put its trust in emerging technology solutions to deliver child protection without rigorous analysis of their flaws, evaluation of the privacy trade-off, and a balancing emphasis on education and awareness." Campaign groups such as the Electronic Frontier Foundation have also argued that the ubiquity of data storage could lead to bad actors selling private information "to data brokers, seized by police or immigration officials, stolen by data thieves, or misused by employees". Beyond the threat of bad actors, age verification methods could create data on browsing habits and internet use likely to be appealing to niche advertisers. There is currently no acceptable or sufficient privacy code governing

	the use of this data by age verification providers, and no provision for this in the Bill. Considering these threats, I urge Ofcom to focus on systems where no new data is created – for example, content filtering at the device or ISP-level (similar to the mobile network operator) option in the guidance should be recommended. Should other forms of age verification technology be recommended, I urge Ofcom to follow a similar approach to the government's announcement on end-to-end encryption, that technology should only be implemented when ready and proven.

Question	Your response
Question 4: Do you agree that service providers should use the proposed criteria to determine whether the age assurance they implement which is highly effective at correctly determining whether or not a user is a child? Please provide any information or evidence in support of your views.	Confidential? – Y / N While the age assurance technologies proposed in the draft guidance could be implemented and several may effectively verify the ages of users, we are not confident that the Act will be as effective as assumed in Parliament. Therefore failing in its stated aims to improve online safety. The issue of children accessing potentially harmful material online requires a societal response. There is no technological solution that will tackle the root causes of the issue of children's safety online. Any attempt by a regulator will be unlikely to succeed without an accompanying focus on education, a call also made by the British Computer Society. This means a proper digital literacy programme (which Ofcom can champion), guidance on relationships and sex education as it relates to online content and in the context of championing communication, consent and respect (which Ofcom can curate) and greater support to caregivers (which Ofcom can encourage).

Question	Your response
Question 5: Do you have any information or evidence on the extent of circumvention risk affecting different age assurance methods and/or on any steps that providers might take to manage different circumvention risks for different methods?	Confidential? – Y / N Already, there are multiple ways for individuals to use technology to freely explore the internet in a privacy-preserving manner, including through the use of VPNs and other security technologies. Accessing and using such technology is relatively easy – especially for technologically literate young people. Age verification will simply create an 'age-gate' to accessing adult content. All it will take for content to be downloaded, accessed and shared by under-18s is for them to use easily available technologies like VPNs (which make it appear that a user is accessing a website from another country) or simply to visit access the 'Dark Web' through the Tor browser. In the latter, there is the risk that young people encounter more dangerous material and could even be exposed to criminal content and interactions. With the prevalence of these technologies, it is likely the effectiveness of age verification systems at the website level, will be limited. At the same time, enforcing such solutions risks creating even greater harm to young and otherwise vulnerable people. It is important to note that VPNs and other IP masking technologies are also a social good in many cases and for some content creators a vital safety tool. Efforts that stop people from being able to find and access them could lead to content creators having their locations revealed and their physical safety threatened.
Question 6: Do you agree with our proposed guidance that providers should consider accessibility and interoperability when implementing age assurance? Please provide any information or evidence in support of your views.	Confidential? – Y / N

Question	Your response
Question 7: Do you have comments on the illustrative case study we have set out in the guidance? Do you have any supporting information or evidence relating to additional examples of how the criteria and principles might apply to different age assurance processes?	Confidential? – Y / N
Question 8: Do you agree with our proposed guidance on the record-keeping duties? Please provide any information or evidence in support of your views.	Confidential? – Y / N
Question 9: Do you have any comments on our proposed approach to assessing compliance with the duties on service providers who publish or display pornographic content, including on the proposed examples of non-compliance? Please provide any information or evidence in support of your views.	Confidential? – Y / N
Question 10: Do you have any comments on the impact assessment set out in Annex 1? Please provide any information or evidence in support of your views	Confidential? – Y / N The Act also creates a significant risk of 'outing' LGBTQ+ people, who access websites that will now need to verify their identities. Protecting their real-life identities allows LGBTQ+ people to share their experiences and sexuality while protecting their privacy. Putting this at risk poses a direct threat to their safety and creates a serious issue for those who, for whatever reason, are not public about their sexual and gender identities. While it may also not be the intention of this regulation to place non-pornographic material that is connected to sex behind strict age-gates, there are countless examples of material related to female sexuality and LGBTQ+ experiences being incorrectly marked as 'porn' as well as loud campaign groups bent on arguing for this.

Question	Your response
	It is deeply concerning that this impact is lacking from Annex 1.
Question 11: Do you agree that our proposed guidance is likely to have positive effects on opportunities to use Welsh and treating Welsh no less favourably than English? If you disagree, please explain why, including how you consider the proposed guidance 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.	Confidential? – Y / N

Please complete this form in full and return to Part5Guidance@ofcom.org.uk.