Consultation response form

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

Consultation title	Consultation: Protecting children from harms online
Organisation name	Yoti

Your response

Question	Your response
Volume 2: Identifying the services children are using Children's Access Assessments (Section 4).	
Do you agree with our proposals in relation to children's access assessments, in particular the aspects below. Please provide evidence to support your view. 1. Our proposal that service providers should only conclude that children are not normally able to access a service where they are using highly effective age assurance? 2. Our proposed approach to the child user condition, including our proposed interpretation of "significant number of users who are children" and the factors that service providers consider in assessing whether the child user condition is met? 3. Our proposed approach to the process for children's access assessments?	Confidential? – N **About Yoti** Yoti is a digital identity company that makes it safer for people to prove who they are. Founded in April 2014, we started by creating a secure Digital ID app which gives people a safer and instant way to prove their identity, with no need to show identity documents or share an excessive amount of personal data. Yoti now provides verification solutions across the globe, spanning identity verification, age verification, age estimation, eSigning and authentication. We're a team of over 400 people, working together to shape the future of digital identity. We're committed to making the digital world safer for everyone. Our seven ethical principles guide us in everything we do and we're held accountable by our independent Guardian Council, whose minutes we publish. With an award-winning social purpose strategy, we're always looking for new ways to explore what (digital) identity means globally. The journey isn't one we're making alone, but with the help of policy advisers, think tanks, researchers, humanitarian bodies and everyday people. What we are doing and why: ● Transforming the way individuals can prove their age and identity ● Increasing security and privacy of personal data ● Helping to create age-appropriate experiences and safer communities online ● Creating the most reliable and comprehensive identity verification solutions ● Shaking up the way we sign documents Technology as a force for good - Yoti was founded on seven business principles which guide our actions. Yoti is also a founding UK B Corp meaning we aim to balance profit with purpose.

Question	Your response
	Security credentials - We commission regular external audits of our business and have been certified to meet some of the world's most stringent security standards, such as ISO 27001 and SOC2 Type II. We are also certified by the UK Government under the UKDIATF (UK Digital Identity & Attributes Trust Framework). A transparent, open and honest approach - Yoti publishes regular white papers to build trust and understanding of our technology. Yoti has conducted over 650 million age checks; hence we bring the benefit of that experience to our response. We already offer age assurance checks at a variety of ages 18+, 25+, 13-17 and under 18. **Children's access** The consultation seems to solely focus on access to 18 plus services. The consultation does not appear to enforce the minimum age required by a platform's terms of service which is often 13, or the age of digital consent. We strongly disagree with the position that 'age assurance does not work well for children' or that there is not evidence that age assurance at 13 is technically reliable, with fall back options available[1]. In pages 16-21 we will detail that age assessment, under the age of 18 and specifically at the age of 13 is already technically reliable and operational today. Ofcom is a trusted regulator. By stating publicly in the consultation and the media, that age assurance of minors, including facial age estimation, is limited or insufficient is implying to the public that the evidence Ofcom has supporting that statement is available and must be convincing. However, Ofcom has not as yet referenced what evidence they have chosen to rely upon to make that judgement, particularly when Yoti's published white paper evidence, contradicting that statement has been available for 5 years. Hence, we look to Ofcom to either publish the supporting evidence that proves that age assurance for under 18s is not reliable or to retract or qualify their current view to explain why the evidence provided, from Yoti and other facial age estimation vendors', is not deemed credible. We would encourage Ofcom to work with the ISO age assurance standard group to set an appropriate level of assurance for 13 age assurance, which may be set at 'Broadly Effective Age Assurance' rather than a higher 'HEAA', where the level of risk is deemed either lower or it is deemed disproportionate to require the higher level of assurance. It is also obviously possible at relatively low cost, for a large regulator, to independently test facial age estimation reliability for the required child ages.

[1] 13.75 that *'limited existing technologies that can reliably identify children of different ages'* and that *'given these limitations, [Ofcom's] proposals focus at this stage on setting the expectation of protections for all children under the age of 18'*

Question	Your response
	Use of *'highly effective age assurance'* (HEAA) We welcome Ofcom's initial proposal, however we would like to see a much clearer, numerical definition of what constitutes *'highly effective'* age assurance included in the guidance. The current guideline criteria of *'technical accuracy, robustness, reliability, and fairness'* require numerical definition. We are also supportive of the approach which consists in solely allowing service providers to *'conclude that it is not possible for children to access a service'* if the *'highly effective'* age assurance is used *'with the result that children are not normally able to access'* the service. We have made a recommendation with regards to the use of the word 'normally' in this sentence in the *'Child assessments'* section of our feedback, below. We support the statement that *'it is unlikely that forms of age assurance which are not highly effective at determining whether a particular user is a child or adult would be able to ensure children are not normally able to access the service or relevant part of it.*' However the above statement also relies on providing clarity as to the definition of *'highly effective'*. We welcome Ofcom's approach to assess *'the alternative approach of not specifying the type of age assurance for children's access assessments, leaving it to the discretion of service providers'*. We agree with the conclusion that this approach could have *'risked potentially leaving children vulnerable to harm if ineffective age assurance is implemented by a provider'*. Other regulators around the world including in Ireland (*Draft Online Safety Code*, Coimisiún na Meán, 27 May 2024, France Arcom Public Consultation on AV, [2] and Australia (*Roadmap for age verification*, eSafety Commissioner, March 2023, and *Children easily bypassing age verification online, putting them at risk of abuse, eSafety commissioner says*, ABC News, 4 September 2023) have all concluded that the most commonly used form of age assurance, self-declaration, is ineffective. **'Significant number' of children** We note that in 4.25, Ofcom '[does] *not propose a numerical threshold for "significant number of children'*. We also note and agree with the fact that Ofcom considers that *'even a relatively small absolute number or proportion of children could be significant in terms of the risk of harm to children'*. We also note Ofcom's statement that *'it cannot be the intention of Parliament that the concept of a "significant number of children" within the meaning of the Act should require the number in question to be a large or substantial number'* and that *'a service of a kind likely to attract a relatively small number of children could still meet this criterion*'. Nonetheless, we do not think Ofcom's statement that the term *'significant number'* should be understood *'as indicating that the number of children on the service is material in the context of the service in question (i.e. not insignificant in that context)'* is sufficiently clear at this stage. We also view the criterias of *'appeal'* and linkage to *'revenue stream'* to also be subjective as currently set out. As we stated in our

[2] ('*Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques*, Arcom, April 2024)

Question	Your response
	response to Ofcom's consultation on its guidance for service providers publishing pornographic content, we would also point to the Information Commissioner's Office *'Likely to be accessed impact assessment'*[3] document published in July 2023 [4], which also references the *'significant number'* threshold. We would like to see both regulator's definitions aligned. **Child assessments** We welcome the inclusion of a duty for providers to consider *'whether it is possible for children to access the service or a part of it'* during *'Stage 1'* of the children's access assessment process.. Equally, we welcome the inclusion of the possibility for providers 'to conclude that it is not possible for children to access a service, or a part of it' only *'if it is using age assurance with the result that children are not normally able to access it'*. Our comment centres around the word *'normally'*. We believe that Ofcom should be clearer in its guidance, and offer service providers with more information about how to quantify *'normally'*, and in particular how they should assess childrens' level of technology literacy and use of circumvention techniques and technologies. Taking the example of Virtual Private Network (VPN) technology, a study by Forbes[5] evidences that younger Britons are more likely to be familiar with this technology and utilise it to bypass online safety measures. (*'18 to 24-year olds have a high level of understanding, with 70% fully grasping the purpose of VPNs, and an additional 17% having a basic recognition of their existence. The 25 to 34 age bracket follows a similar pattern, but with a higher VPN awareness rate of 78%. Among this group 41% have a clear understanding of VPNs, while 37% have a more general familiarity. People aged 65 and older have the lowest VPN awareness, but most (57%) still know about them. Overall, 15% understand the purpose of VPNs well, while 42% have some knowledge but lack detailed understanding*.'). According to another article by ExplodingTopics[6] *'the 16-24 demographic makes up 35% of all VPN users'*. We also note Ofcom's own research published in Volume 3 (*'the causes and impacts of online harms to children'*), which highlights that *'the BBFC and Revealing Reality found that 23% of children (aged 11-17) reported knowing how to use a potential 'workaround' (e.g. a virtual private network (VPN), file torrenting, the use of Tor or the 'dark web'). The youngest children (11-13) were the least likely to report knowing how to use any of these functions (14%), compared to the older children – 25% aged 14-15, and 33% aged 16-17*'. Therefore, there is a risk that service providers assume varying levels of technological literacy among children, leading to different conclusions regarding a variety of services. As a result, they may choose not to implement HEAA, concluding that children are not *'normally'* likely to access their service. In addition, video sharing platforms (VSPs) and on-demand programme service (ODPS) providers already block VPNs

[3] ('*Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques*, Arcom, April 2024)

[4] (https://ico.org.uk/media/4025881/ltba-guidance-impact-assessment.pdf)

[5] (VPN Statistics, Forbes, 3 June 2024, https://www.forbes.com/uk/advisor/business/vpn-statistics/)

[6] (30+ VPN Statistics, Trends & Facts (2024-2027), ExplodingTopics, 26 January 2024, https://explodingtopics.com/blog/vpn-stats#vpn-users)

Question	Your response
	effectively by blacklisting the most commonly used IP addresses and detecting new ones based on high traffic volumes. While more expensive VPN services offer less traceable IP addresses, their cost serves as a barrier to children accessing pornography. Additionally, if a child uses a parent's credit card, the payment to the VPN will appear on the statement, giving the parent an opportunity to detect unauthorised activity (*'UK web users to undergo age verification to access porn'*, Biometric Update[7]. On this basis, we encourage Ofcom to proactively review VSPs and ODPSs' approaches to VPNs, applying the insights gained from regulating these services over the past two years to the Online Safety regime. We believe it is important that Ofcom's guidance be more precise regarding children's level of technological literacy, to ensure that providers conduct *'suitable and sufficient'* children's access assessments uniformly. This could be achieved through the publication of research, specific examples of best practice and suggestions. We would make similar recommendations with regards to the use of the word *'possible'* (*'for children to access a service'*). We would suggest that there is a likely problem with dispositions at 4.7 (*'Where a service provider fails to complete a children's access assessment, the service will be treated as likely to be accessed by children*.'). Indeed, there is not currently a duty for service providers to publish the outcome of their children's access assessments. Whilst we recognise that some sections of providers' assessments, such as sections relating to circumvention and potential weaknesses, should not be made public, we would question how Ofcom will be able to know whether a platform has failed to complete one such assessment. As it is likely that many tens of thousands of websites will fall in scope of these dispositions, the process of asking sites to provide the outcome of their assessment could be incredibly time-consuming. Whilst we recognise that it would also be counter-productive to require providers to send their assessments to Ofcom for review (due to how huge a volume of documentation to review this would imply), we would suggest that a sensible middle ground would be to require providers to make the outcome of their assessments publicly available on their site. We would suggest that this approach should be similar to duties for providers to *'include provisions'* that are *'clear and accessible'* (paragraphs A13.96 to A13.100). This means that *'trusted flaggers'* and *'super-complainers'* would be able to access these documents and support Ofcom's work by flagging instances where they disagree with the outcome of an assessment, or where that assessment was missing altogether. We would suggest that section 5.29 (*'Evidence from external/third party sources demonstrating that the service is not likely to attract children. This may include market research and quantitative evidence from third parties that track child media consumption, for example media trackers*.') be rephrased to include the words *'independent'* and *'reputable'* '*external/third party sources'.* Indeed, in its 2024 *'three-year Media Literacy strategy'* consultation Ofcom suggests *'encouraging online services to fund third-party interventions direct to users'*, but also states elsewhere in the text that

[7] 8 February 2022, available at https://www.biometricupdate.com/202202/uk-web-users-to-undergo-age-verification-to-access-porn).

Question	Your response
	'organisations that are funded by platforms and delivering media literacy initiatives or resources face a number of challenges that limit their full potential. These include fragile and short-term funding agreements, a constant pressure for 'new' content, and potentially selective or partial content created to suit brand values rather than user needs.' Therefore, we would welcome suggestions from the regulator on how some of these limitations can be overcome. Further, providers should be made aware that Ofcom would only consider *'evidence from external/third party sources demonstrating that the service is not likely to attract children'*, if this evidence comes from an independent and reputable source. We welcome the statement in 4.41 with regards to the unreliability of age data obtained through *'self-declaration'* or *'online payments methods'*. Whilst we have specific comments about this section, which we have included in the relevant sections of this consultation response (below), we would suggest simplifying this section by clarifying that the only age that can be relied on for children's access assessments is data collected through methods listed as effective in Annex 10 (*'Draft guidance on highly effective age assurance'*) and that were operating to match the HEAA criteria such as in Annex 7 (*'Protection of Children Code of Practice for user-to-user services'*, sub-section *'Highly effective age assurance'*). This is to ensure that service providers understand they may only rely on data obtained through an age assurance method that was functioning correctly at the time of collection and complied with Ofcom's standards. We think section 4.46 (*'Record keeping duties'*) could be clarified to specify that all providers should keep this record, regardless of whether they conclude that children are normally able to access their service in full or in part and that these records should be made publicly available, published on their website. Therefore, we would suggest rephrasing 4.47 to clarify that providers should also keep a written record of their *'detailed evidence-based assessment'*. This should also apply to the *'methodology'* and *'evidence'* used by providers (4.48). We think this should also be available to users as per our general feedback (above in this section). In addition to the record keeping duties, Ofcom could require that larger revenue PC and PPC businesses be independently reviewed every two or three years, to review that the self assessment that minors are not accessing their website is indeed correct. This will enable the regulator to know whether businesses are complying with the law and providing only age appropriate access. In addition the regulator may consider AI compliance scanning tools or mystery shopper visits to test age appropriate access across a much wider set of organisations. It is interesting to consider the parallel in food safety[8], where even small organisations expect visits each 6 months. We note the additional duty for providers who *'have concluded that a service is not likely to be accessed by children'* (4.49, 4.50, 4.51). We would again flag that due to the likely very high volume of providers who will, at least initially, come to such a conclusion, it will be difficult for Ofcom to keep track. Therefore, we would recommend, similarly to our feedback above, that Ofcom

[8] https://www.gov.uk/food-safety-your-responsibilities/food-inspections

Question	Your response
	mandates that providers keep a record of assessments as listed in 4.50, and that these should be made publicly available. We are supportive of provisions as drafted in 4.54. However, we would assume that the spirit of these provisions is to imply that providers would only come across *'evidence about reduced effectiveness of age assurance'* through observing the functioning of their chosen age assurance solution on their platform. We believe that Ofcom should support providers by conducting periodic reviews of the various age assurance solutions employed by providers in scope of the regime, conduct horizon scanning, testing, and publish the results of these alongside updating its guidance on age assurance. This would help reinforce the conclusion in 4.67 ('*carrying out children's access assessments will entail only small or negligible costs in the vast majority of cases, which can be absorbed by service providers including small or micro businesses, and that these costs largely derive from the requirements of the Act')* and support providers who opt to employ third party, external age assurance solutions, and could provide some independent and factual research for providers who opt to develop their own solutions. This would also help service providers better *'to technological developments over time'* (15.300). We will repeat this feedback on the other relevant sections. We recommend that Ofcom mandate independent third-party certification or assessment providers to test the effectiveness of age assurance methods and processes *'for services to understand the effectiveness of their age assurance methods and processes'* (4.55). This will ensure that service providers receive accurate information about their systems. Similarly to the feedback we have provided about Ofcom's approach to defining a *'significant number of children'*, we would like more clarity on what a *'significant increase'* in *'the number of children using the service'* would be (sections 4.57, 4.58. 4.59, '*In response to evidence about a significant increase in the number of children using the service'*). We welcome Ofcom's *'provisional conclusion'* that its proposal on children's access assessments would not *'constitute interference with users' (both children and adults) or services' freedom of expression or association rights*'. As we will emphasise throughout this response, given the likely high number of sites covered by the Act compared to Ofcom's relatively small human resources, this will rely on thorough and consistent regulation and enforcement by the regulator. We would slightly disagree with the assessment that '*more significant direct costs may apply in limited cases where services believe they are not likely to be accessed by children and decide to conduct additional work to establish relevant evidence that demonstrates this, in line with our proposed guidance'* and especially the statement that 'may incur costs associated with gathering the relevant evidence to demonstrate their approach meets the criteria for highly effective age assurance'. This likely will not be true for services which rely on third party age assurance providers such as Yoti, as documentation which evidences the high performance of our technology is ready available on our website at no cost (Facial Age Estimation white paper, Yoti, December 2023, https://www.yoti.com/blog/yoti-age-estimation-white-paper). This is likely to be true for other such third party providers.

Question	Your response
	We welcome the inclusion on this guidance document of '*examples of content types that are appealing to children'*. Similarly and in order to support the aims of 5.20 (*'Children are a part of a service's commercial strategy'*), Ofcom could also include examples of advertising whose *'nature, design, or content'* are *'appealing to children'*. VPN advertising could be one type of advertising deemed appealing to children, as providers are discouraged from promoting it on their platforms according to Ofcom's guidance.
Volume 3: The causes and impacts of online harm to children **Draft Children's Register of Risk (Section 7)**	
Proposed approach: 4. Do you have any views on Ofcom's assessment of the causes and impacts of online harms? Please provide evidence to support your answer. a. Do you think we have missed anything important in our analysis? 5. Do you have any views about our interpretation of the links between risk factors and different kinds of content harmful to children? Please provide evidence to support your answer. 6. Do you have any views on the age groups we recommended for assessing risk by age? Please provide evidence to support your answer. 7. Do you have any views on our interpretation of	Confidential? – N We note that Volume 3 (*'The causes and impacts of online harms to children'*) provides extensive evidence about the importance of considering the risk to children in different age groups of encountering content harmful to children. The document provides a comprehensive overview of the impact of harmful content on children of different age groups. Children aged 0-5 are significantly influenced by parental involvement in their online activities and are at risk of encountering harmful content, especially if they use devices and profiles belonging to other family members. As children aged 6-9 become more independent and nearly all are online, they start to encounter harmful content, such as pornography, with 21% experiencing offensive or hurtful behaviour, primarily through messaging or social media. Children aged 10-12 experience rapid biological and social changes, increasing their online presence and the risk of harmful interactions like bullying, with a shift from direct to more passive parental supervision. Those aged 13-15 use a wider range of online services and are more likely to encounter and seek out harmful content, with exposure to content like suicide and self-harm being particularly impactful due to their vulnerability to mental health issues. Older teens aged 16-17 gain more online independence and are less supervised by parents, increasing their exposure to harmful content as they are more likely to speak to strangers online and use adult profiles, despite parental concern and supervision significantly decreasing for this age group. Viewing harmful content affects children's emotional well-being, causing anxiety, shame, and fear, with specific types of harmful content discouraging self-expression and leading to the normalisation of violent behaviours. At worst, harmful content can contribute to loss of life, with instances of exposure to content promoting suicide and self-harm leading to tragic outcomes, including the suicides of children like Molly Russell and Mia Janin. Vulnerable groups, including children needing mental health support, neurodiverse children, and those with mental health conditions, are particularly susceptible to encountering and being adversely affected by harmful content depicting violence and promoting harmful behaviours.

Question	Your response
non-designated content or our approach to identifying non-designated content? Please provide evidence to support your answer. **Evidence gathering for future work:** 8. Do you have any evidence relating to kinds of content that increase the risk of harm from Primary Priority, Priority or Non-designated Content, when viewed in combination (to be considered as part of cumulative harm)? 9. Have you identified risks to children from GenAI content or applications on U2U or Search services?	Among much feedback, we note Ofcom's conclusion in 7.1 (Pornographic content) that *'pornographic content is pervasive in the online lives of children. Most children encounter pornographic content online by their mid-teens, with one in ten encountering it before the age of 9. The impact can vary between individuals, but evidence indicates that attitudinal, psychological and behavioural impacts exist. For example, the normalisation of violent sexual behaviours can affect children's attitude to sex and relationships'*. We also note that *'the average age at which children first encounter pornography is 13, although older children (14-17) are more likely to see it regularly. Across all ages, boys are more likely to encounter pornography than girls*.' Finally, as specified in 7.1.1, we note that the Online Safety Act 2023 requires services to consider *'the level of risk of harm to children presented by different kinds of content that is harmful to children, giving separate consideration to children in different age groups'*. We also note the point made in 7.11.19 that *'the absence of robust age assurance systems and processes, or a strategy on how to effectively identify child users, may increase the risk of harm to children'*. We would recommend that Ofcom undertake extended dialogue with a range of stakeholders to understand the threats to children in immersive online environments. This includes environments which rely on the use of haptics or shared headset devices, which make it harder for a parent to see what content a child is encountering. Some useful resources on this topic, which Ofcom should consider reviewing, are detailed below[9]: We would also encourage ongoing review of Nudify apps and more stringent requirements for consent and confirmation of age at the point of uploading content, from the content uploader and other individuals within content, to deter deepfake and non consensual image abuse. It would be helpful if payment processors were required to provide transparency reports, detailing how they

[9] *The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse*, Manchester University, available at: https://documents.manchester.ac.uk/display.aspx?DocID=62042 and https://blog.policy.manchester.ac.uk/posts/2022/06/online-safety-child-abuse-and-exploitation-in-extended-reality/; *Metaverse: Potentials for Exploitation by Child Sexual Offenders*, University of Bath; *Beginners Guide to VR*, Upload VR, available at: https://uploadvr.com/beginners-guide-vr-faq-everything-you-need-to-know/; *Virtual Reality and Augmented Reality, Refresh Science*, available at: https://refreshscience.com/virtual-augmented-reality-ppt/; *Virtual Reality for Kids: Parents Guide (2021),* Smart Glasses Hub, 2021, available at: https://smartglasseshub.com/vr-for-kids/; *First Responder XR,* Sprite, 2021, available at: https://spritehub.org/2021/08/20/first-respondxr-digital-vulnerability-of-immersive-training-for-first-responders/; *What is a Metaverse?,* Gartner, available at: https://www.gartner.com/en/articles/what-is-a-metaverse; *The Metaverse Value Chain*, Jon Radoff, available at: https://medium.com/building-the-metaverse/the-metaverse-value-chain-afcf9e09e3a7; *Safeguarding in The Metaverse*, IET, available at: https://www.theiet.org/impact-society/factfiles/information-technology-factfiles/safeguarding-the-metaverse/.

Question	Your response
a) Please Provide any information about any risks identified 10. Do you have any specific evidence relevant to our assessment of body image content and depressive content as kinds of non-designated content? Specifically, we are interested in: a) (i) specific examples of body image or depressive content linked to significant harms to children, b. (ii) evidence distinguishing body image or depressive content from existing categories of priority or primary priority content. 11. Do you propose any other category of content that could meet the definition of NDC under the Act at this stage? Please provide evidence to support your answer.	monitor adherence to their practices in this regard. An example of such practice includes guidelines published by Mastercard in 2021[10]. Some requirements updated in this guidance include documenting age and identity verification for all individuals depicted and those uploading the content, implementing a content review process before publication and establishing a complaint resolution process that addresses illegal or non consensual content within seven business days. A report from the Internet Watch Foundation[11] found over 11,000 potentially criminal AI-generated images of children on one dark web forum dedicated to child sexual abuse material (CSAM). They assessed around 3,000 images as criminal. The IWF has found *'many examples of AI-generated images featuring known victims and famous children'*. Generative AI can only create convincing images if it learns from accurate source material. Essentially, AI tools that generate CSAM need to learn from real images featuring child abuse.
Draft Guidance on Content Harmful to Children (Section 8)	

[10] (*'Protecting our network, protecting you: Preventing illegal adult content on our network'*, Mastercard, https://www.mastercard.com/news/perspectives/2021/protecting-our-network-protecting-you-preventing-illegal-adult-content-on-our-network/)

[11] ('*How AI is being abused to create child sexual abuse imagery'*, October 2023, available at https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf)

Question	Your response
12. Do you agree with our proposed approach, including the level of specificity of examples given and the proposal to include contextual information for services to consider? 13. Do you have further evidence that can support the guidance provided on different kinds of content harmful to children? 14. For each of the harms discussed, are there additional categories of content that Ofcom a) should consider to be harmful or b) consider not to be harmful or c) where our current proposals should be reconsidered?	No comment.
Volume 4: How should services assess the risk of online harms? **Governance and Accountability (Section 11)**	
15. Do you agree with the proposed governance measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and explain your views and provide any	Confidential? – N We note that as part of its *'core inputs'* and in table 12.3 (*'Considerations for core inputs'*), Ofcom writes that *'the Act requires services to consider their user base, including the number of users who are children in different age groups as part of the children's risk assessment process. Services should therefore assess their risks based on relevant user data. According to the Act, user data includes "(a) data provided by users, including personal data (for example, data provided when a user sets up an account), and (b) data created, compiled or obtained by providers of regulated services and relating to users (for example, data relating to when or where users access a service or how they use it)." We consider that user data would include any data held as a result of age assurance and age*

Question	Your response
arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 16. Do you agree with our assumption that the proposed governance measures for Children's Safety Codes could be implemented through the same process as the equivalent draft Illegal Content Codes?	*verification processes'*. We also note that the corresponding *'benefits'* section of table notes that this type of information could include *'data from age assurance processes; data from self-declaration; proxy indicators for age, such as behavioural patterns identified while a user is active on the service which gives a reasonable indication of age'*. We agree that for self-declaration, *'data of this kind is likely to have limited accuracy and services should not place excessive reliance on it, including because of known tendencies for some children to provide inaccurate data'* and that *'providers should not therefore rely on it for assessing the numbers of users who are children in the context of children's access assessments'*. But the guidance also states that *'however, this evidence, in combination with other kinds of information, or as a way of estimating a lower bound for the possible number of children on the service, can be a helpful consideration as part of the children's risk assessment, to help services make judgments regarding children in different age groups on their service and the risk level they face'*. Therefore we would flag the potential risk of over-collection of data, particularly when services collect precise details such as the exact age and date of birth rather than simply determining whether a user is a child. We urge Ofcom to make it clear to providers that they should limit data collection to what is necessary to determine if a user is a child. Exact age and date of birth should not be collected unless absolutely necessary. Additionally, users should be transparently informed about what data will be collected, how it will be used, and the purpose for which it is being collected, with clear justification provided. This approach will help protect children's privacy while ensuring compliance with the Act. It is essential for providers to balance the need for accurate age verification with the minimisation of data collection to safeguard children's privacy and adhere to data protection principles.
Children's Risk Assessment Guidance and Children's Risk Profiles' (Section 12)	
17. What do you think about our proposals in relation to the Children's Risk Assessment Guidance? a) Please provide underlying arguments and evidence of efficacy or risks that support your view. 18. What do you think about our proposals in relation to the Children's Risk Profiles for Content Harmful to Children?	No comment.

Question	Your response
a) Please provide underlying arguments and evidence of efficacy or risks that support your view. Specifically, we welcome evidence from regulated services on the following: 19. Do you think the four-step risk assessment process and the Children's Risk Profiles are useful models to help services understand the risks that their services pose to children and comply with their child risk assessment obligations under the Act? 20. Are there any specific aspects of the children's risk assessment duties that you consider need additional guidance beyond what we have proposed in our draft? 21. Are the Children's Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service? a) If you have comments or input related to the links between different kinds of content harmful to children and risk factors, please refer to Volume 3: Causes and Impacts of Harms to Children Online which	

Question	Your response
includes the draft Children's Register of Risks.	
Volume 5 – What should services do to mitigate the risk of online harms **Our proposals for the Children's Safety Codes (Section 13)**	
Proposed measures 22. Do you agree with our proposed package of measures for the first Children's Safety Codes? a) If not, please explain why. **Evidence gathering for future work.** 23. Do you currently employ measures or have additional evidence in the areas we have set out for future consideration? a) If so, please provide evidence of the impact, effectiveness and cost of such measures, including any results from trialling or testing of measures. 24. Are there other areas in which we should consider potential future measures for the Children's Safety Codes? a) If so, please explain why and provide supporting evidence.	Confidential? - N We note Ofcom's statement that it *'will not take enforcement action against them for breach of that duty if [the measures recommended in Ofcom's Children's Safety Codes] have been implemented'*. In order to support Ofcom in its work, and in particular that of *'trusted flaggers'* and *'super complainers'*, we would reiterate our feedback provided to Volume 2 (*'Identifying the services children are using'*), and in particular about the opportunity to clarify section 4.46 (*'Record keeping duties'*) to specify that all providers should keep the record, regardless of whether they conclude that children are normally able to access their service in full or in part, as well as rephrasing 4.47 to clarify that providers should also keep a written record of their *'detailed evidence-based assessment'*. This should also apply to the *'methodology'* and *'evidence'* used by providers (4.48). We think this should also be available to users publicly as per our general feedback (above in this section). **Use of *'highly effective age assurance'* (HEAA).** We support Ofcom's proposition in 13.24 ('*Understanding which users are children so they can be protected online')* that *'highly effective age assurance'* should be *'age assurance that is highly effective at correctly determining whether or not a user is a child'*. Whilst we agree that *'age assurance is not a silver bullet',* we would nonetheless highlight that *'highly effective'* age assurance, once adequately defined with specific numerical thresholds will certainly be the cornerstone of the Online Safety regime. The regime is largely focused on protecting children from harm and relies on the feasibility and success of various safety measures proposed in Ofcom's guidance. **Broadly effective Age Assurance** However, as per page 3, we would advocate that Ofcom also selects a level of assurance in conjunction with the ISO standard working group, perhaps termed 'Broadly Effective Age Assurance to meet the risk profile to enable age assessment to meet terms of service at the age of 13. This concept of various levels of risk based assurance e.g. high, medium, low depending on the user case - is well established in identity assurance. We would like to offer comprehensive feedback to Ofcom's *'Draft guidance on highly effective age assurance'* (Annex 10). We will, for the most part, reiterate the feedback we have provided in our

Question	Your response
	response to Ofcom's previous *'Guidance for service providers publishing pornographic content'* consultation. Our feedback on the criteria is that the *'technical accuracy'*, *'robustness'*, and *'reliability'* sections appear confluent, largely describing the same aim: ensuring that the age assurance method accurately determines a person's age. We suggest merging these into a single *'precision'* criterion and aligning these to the international standards workstream outputs in terms of specific percentages. Additionally, as mentioned in our response to a previous consultation (*'Protecting people from illegal harms online'*), we believe that the ease of circumvention of measures, the evolution of circumvention techniques (such as virtual private networks), and users' literacy levels in this field have been inadequately addressed in the documentation, aside from a duty on service providers not to promote them on their sites. These factors are crucial when assessing and implementing an age assurance solution and should form the basis of a criterion. We would welcome formal studies in this field. We also recommend renaming the *'fairness'* criterion to *'equity'*, as *'fairness'* does not seem the best term in this context. We are aware that a number of regulators, international organisations and global firms use different scales such as the Fitzpatrick scale, the Monk scale, and NIST's country-based scale. Each of those scales present a number of advantages, but there is an ongoing global debate as to which, or which combination of scales, should be used. We would encourage Ofcom to work on securing a global consensus, perhaps through the GOSRN, on which scale or combination of scale should be used globally. For this criterion, Ofcom could encourage the use of proxies for skintone, such as means to assess country of origin (eg via country code) or use of measures such as the Fitzpatrick scale, as used in Yoti's *'Facial Age Estimation White Paper'* (Facial Age Estimation white paper, 15 December 2023, available at https://www.yoti.com/blog/yoti-age-estimation-white-paper/). The Fitzpatrick scale is a dermatological test grading skin tone at two different points in time, before and after a week's sun exposure. It could also be useful if more detail were published by Ofcom to review the utility of the Monk Skin tone scale[12]. . Ofcom should be more thorough in its guidance in this section to mitigate the potential harms identified in other sections of the guidance. Providers need to assess whether the datasets used by age assurance technology providers to train their algorithms are ethically sourced and representative of the broader UK population. Conducting socio-demographic reviews would also be valuable, for example, to assess whether there are inequalities in access to various age assurance methods, such as those that rely on credit cards. In the US, the Federal Reserve Board published a report (*'Economic Well-Being of U.S. Households in 2022'*, Board of Governors of the Federal Reserve System, May 2023) looking at the economic well-being of households, including data on credit card access. 82% of adults in the US own a credit card. But this falls to 62% of younger adults, aged between 18 and 29. In the United Kingdom, research suggests this number for the overall

[12] ('Improving skin tone representation across Google
Google, May 2022, available at https://blog.google/products/search/monk-skin-tone-scale/)

Question	Your response
	population is around 65-68%, and has declined in recent years. The Federal Reserve's report concluded that credit card usage also differs by race, ethnicity and disability status. Income data from employment, savings and investments are the most influential factors in determining whether a credit card is issued or not. But it's fair to say that more adults who are from certain racial or ethnic groups, or have a disability, face discrimination if a regulation or organisation requires evidence of credit card ownership to access a service. It is also important to note that adults on lower incomes will find it harder to qualify for a credit card. These same adults may also struggle to buy other forms of identification, such as a passport, which can be expensive. It is crucial to know who is in possession of a document being presented. Furthermore, Ofcom should add two additional considerations for service providers when reviewing solutions (in 4.37). First, whether the solution poses any barriers to users reliant on possessing a document, or device, thus excluding a segment of the population. This is relevant considering the cost and complexity of obtaining identity documents or modern devices. Providers should consider implementing several age assurance technologies to provide users with a choice, mitigating this risk. Users should always have a choice of age assurance methods. Additionally, there should be a section on 'inclusivity' alongside 'accessibility' as core criteria for highly effective age assurance (Figure 4.1, A10.1, *'Summary of our approach to implementing highly effective age assurance'*). The *'accessibility'* section currently lacks detail. Given that 24% of the population has a disability[13] , the guidance should use the word *'must'* rather than *'could'* for this section (*'Principles that service providers should have regard to'*). We would like to see references to accessibility standards, principles, and techniques such as the Children's Code, the Hemingway system of *'grade level'* judging in terms of the review of language used, and the Web Content Accessibility Guidelines (WCAG). Age assurance technology providers should aim to achieve a minimum level of WCAG 2.2 (Yoti achieved this in July 2023), with assessments conducted by an independent third party, ensuring true independence as assessors are compensated regardless of the outcome. **Children in different age groups** We welcome Ofcom's suggestion in 13.61 that it is *'exploring more tailored protection strategies for different age groups*.' This aligns with all the evidence presented regarding the varying impact of harms on children based on their age group in Volume 3 (*'The causes and impacts of online harm to children'*). However, we do not understand the decision that Ofcom has spelt out in 13.74, 13.75, and 13.76. We would highlight that the *'Age-appropriate experiences for children online'* section of the '*Online Safety Act: explainer'* webpage states the following: '*The strongest protections in the Act have been designed for children and will make the UK the safest place in the world to be a child online.*

[13] (*'UK disability statistics: Prevalence and life experiences'*, House of Commons Library, 23 August 2023)

Question	Your response
	Platforms will be required to prevent children from accessing harmful and age-inappropriate content. The Act requires social media companies to enforce their age limits consistently and protect their child users. Services must assess any risks to children from using their platforms and set appropriate age restrictions, ensuring that child users have age-appropriate experiences and are shielded from harmful content. Websites with age restrictions need to specify in their terms of service what measures they use to prevent underage access and apply these terms consistently.' It further states that *'companies can no longer say their service is for users above a certain age in their terms of service and do nothing to prevent younger children accessing it.'* [14] In addition, as we have highlighted in our response to questions in this consultation with regards to Volume 3 (*'The causes and impacts of online harm to children'*), we disagree that there is *'currently limited evidence on the specific impact of harms to children in different age groups'*. Volume 3 provides substantial evidence on the importance of assessing risks for children in different age groups regarding harmful online content. The document outlines that children aged 0-5 are at risk mainly through indirect exposure via family devices, while those aged 6-9 begin to encounter harmful content like pornography and hurtful behaviour as they become more independent online. For children aged 10-12, the risk increases due to rapid developmental changes and less direct parental supervision, leading to higher chances of bullying and harmful interactions. Teenagers aged 13-15 are particularly vulnerable to self-harm and suicide-related content due to their greater online activity and mental health sensitivity. Older teens, aged 16-17, face the highest risks as they navigate the internet with minimal parental oversight, exposing them to a broader range of harmful content. The document emphasises that viewing harmful content significantly impacts children's emotional well-being, causing anxiety, shame, and fear, and can lead to the normalisation of violent behaviours. The document highlights tragic cases, such as the suicides of Molly Russell and Mia Janin, to underscore the potential severity of exposure to harmful content. Vulnerable groups, including children needing mental health support, neurodiverse children, and those with mental health conditions, are especially susceptible to negative impacts from online harm. This comprehensive overview stresses the necessity for tailored risk assessments and protective measures for children across various age groups to mitigate these risks effectively. Secondly, we would like to express our strong disagreement with the statement made in 13.75 that *'limited existing technologies that can reliably identify children of different ages'* and that *'given these limitations, [Ofcom's] proposals focus at this stage on setting the expectation of protections for all children under the age of 18'*. We would express our equally strong disagreement with statements made by Ofcom's Chief Executive Officer Dame Melanie Dawes DCB during an interview on *Today* (BBC Radio 4) on 14 June 2024 [15](*'So you're absolutely right, we haven't said that we're requiring age assurance at age 13. (...) One of the reasons is that these age assurance technologies - which scan your face & estimate your age, and don't ask for any other details, but do estimate your*

[14](https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#:~:text=The%20Act%20requires%20social%20media,are%20shielded%20from%20harmful%20content)

[15] https://www.bbc.co.uk/sounds/play/m00202r1 at 1hr 13min 50secs

Question	Your response
	age, don't work very well on children, as children can look so different at different ages, as I'm sure we'll all know'). We believe the statements made, both in this consultation document and in the media are incorrect. There is a robust ecosystem of providers offering facial age estimation services. Several providers, including Google, have undergone review by the Age Check Certification Scheme (ACCS) and are listed on its registry[16]. Others have been assessed through the NIST global benchmark of facial age estimation or are approved on Germany's KJM Raster of age assurance methods. Despite the dataset's limited diversity (primarily from immigration checks at one country, Mexico) and the absence of mobile phone-captured data, the US NIST's Facial Age Technology Evaluation (FATE) report from May 2024 underscores the effectiveness of vendors such as Yoti and Incode in accurately determining whether younger children are under or over 13 or 18, as indicated by their Mean Absolute Error (MAE) and False Positive Rate (FPR) results. NIST expects continued enhancements in Facial Age Estimation (FAE) based on their extensive experience with Facial Recognition accuracy over the past decade. We have prepared a 30-minute video outlining NIST FATE benchmark results for interested parties (https://vimeo.com/963138932/a0b52b9da0?share=copy). Yoti's Facial Age Estimation (FAE) technology has been publicly providing scientific data on facial age estimation for over 5 years. This comprehensive dataset includes gender-specific and year-by-year estimations from ages 6 to 70, which contrasts with claims made by Ofcom. Yoti's latest age estimation is publicly available[17] . Yoti's Facial Age Estimation achieves significant accuracy levels. It can estimate 65% of children aged 6 - 17 within the correct year or within 1 year either side. Additionally, it accurately estimates 85% within the correct year or within 2 years either side. The parallel well trusted in the offline world; is that a teacher with longstanding experience would be broadly effective at assessing children, unknown to them, into age groups such as 3-5, 8-10 olds and 13-14 year olds. This is clearly possible and helpful to assist in building age appropriate settings. The state of the art facial age estimation brings this human estimation skill up to date and is even more accurate. This level of accuracy is crucial for designing age-appropriate online experiences. For example, Yoti's independently audited White Paper reports a 99.91% True Positive Rate for identifying children aged 5-7 as under 13. In the UK, where there are around 3.62 million children aged 8-12 and 2.17 million aged 13-15, employing a 13.0 age threshold with Yoti FAE reveals that 95.8% of 8-12 year olds are effectively restricted from accessing content meant for 13+ users, and 91.1% of 13-15 year olds are appropriately granted access.

[16] https://accscheme.com/registry/

[17] (*Facial Age Estimation white paper,* 15 December 2023, https://www.yoti.com/blog/yoti-age-estimation-white-paper/)

Question	Your response
	Parents show a heightened concern regarding children accessing age-inappropriate content online. Specifically, they are more apprehensive about 10-12 year olds accessing material intended for adults aged 18 and above, compared to older teenagers aged 16-17. Similarly, there is greater unease about 8-10 year olds using social media platforms meant for users aged 13 and older, in contrast to 12 year olds. Ofcom could consider establishing an age threshold of 15 to reduce the possibility that roughly 1.1% (approximately 39,875) of older 8 - 12 year olds could access content meant for 13-year-olds and above. Nevertheless, such a threshold would also prevent approximately 75% of 13 - 15 year olds and some younger-looking 16-17 year olds from accessing this content, necessitating alternative age verification methods. The data highlights the effectiveness of Yoti FAE in age assessing for the majority of 8 to 15 year olds accessing content intended for those aged 13 and above, both within the UK and internationally. This is the case despite ongoing preferences from regulators and parents for even higher levels of accuracy. Whether the current performance of Yoti FAE can be considered sufficiently 'highly' effective for age assessing access to 13+ content remains subject to interpretation, pending a clear definition. The question is whether FAE is adequate to enhance overall outcomes for age assessment to access 13+ content. Arguably so, particularly if other methods continue to allow too many younger children to access potentially harmful or inappropriate content. Yoti FAE is also recognised for its resilience against spoofing, unlike some other age assurance methods. While some regulators may favour verified date of birth checks to eliminate the risk of approximately 6% of 8- 15 year olds being inaccurately estimated as under or over 13, such methods pose challenges, are costly, and may be exclusionary in many countries. Some people point to parental verification as an answer; however surveys show that a significant percentage of parents admit to complicity when their child lies about their age (*'A third of children have false social media age of 18+'*, published by Ofcom, January 2024[18],) or that many parents do not manage to engage with parental controls. Yonder Consulting research, for Ofcom[19], states that 6 in 10 (60%) children aged 8 to 12 who use these platforms are signed up with their own profile. Among this underage group (8 to 12s), up to half had set up at least one of their profiles themselves, while up to two-thirds had help from a parent or guardian. A study by insurer Aviva[20] (*'1.5 million UK 10-15-year-olds could be exposed to online risks at home'* found that more than a third of UK parents (34%) with children aged 10-15 allowed their children to use the internet without any parental controls. Only eight per cent of respondents said they actually supervised

[18]https://www.ofcom.org.uk/online-safety/protecting-children/a-third-of-children-have-false-social-media-age-of-18/

[19]https://www.ofcom.org.uk/online-safety/protecting-children/a-third-of-children-have-false-social-media-age-of-18/

[20] Aviva, January 2017, https://www.aviva.com/newsroom/news-releases/2017/01/uk-15-million-uk-10-15-year-olds-could-be-exposed-to-online-risks-at-home-17727/)

Question	Your response
	their children while online. The Washington Post[21] reports low levels of parental engagement with supervision settings, 'by the end of 2022, fewer than 10 percent of teens on Meta's Instagram had enabled the parental supervision setting, according to people familiar with the matter who spoke on the condition of anonymity to discuss private company matters; of those who did, only a single-digit percentage of parents had adjusted their kids' settings. Internal research described extensive barriers for parents trying to supervise their kids' online activities, including a lack of time and limited understanding of the technology'. For items restricted to those aged 18 and over, such as alcohol or knives, regulators could consider higher age thresholds, such as 23 (with a 5-year buffer) or 25 (with a 7-year buffer), to further restrict access among 15-17 year olds to less than 0.5% or 0.2%, respectively. The mean absolute error in age estimation is smaller for children than for adults. As individuals age, differences in self-care widen, making it more challenging to accurately assess adults' ages compared to children. We welcome the inclusion of Yubo as an example of best practice in Ofcom's Volume 5 document (*What should services do to mitigate the risks of online harms to children?,* 15.38, *'Yubo is a service targeted at children and young people. It uses Yoti, a third-party solution based on facial age estimation to check user age, supported by identity verification where an age estimation result requires additional checks*.') Indeed, Yubo has successfully implemented an age assessment approach for several years. They categorise users into groups for 13 - 17 year olds and 18+ users, using facial age estimation initially for registration triage. They offer fallback options like digital ID (such as a PASS Card), document uploads, or customer support validation through methods like birth certificates or video interviews with a parent or guardian. Data published by the Office for National Statistics[22] estimates that about 75% of 13 year olds, or 7,219.650 children, own a UK or non-UK passport. ONS data[23] also shows there are 9,654,163 children aged 0-13 in the UK, which implies that 74.8% of children own a passport by the age of 13 . In Scotland, children can obtain the Young Scot Card for free starting from age 11. An under-16 CitizenCard could be provided to those wrongly estimated as 13, offering an alternative for those without passports. This could potentially include means-testing, with provisions for children receiving free school meals. Additionally, exploring vouching systems by teachers or other professionals could be considered, drawing from approaches adopted by the National Proof of Age Standards Scheme (PASS) and CitizenCard. We propose that Ofcom convene an industry workshop on this topic, which we would support.

[21](https://www.washingtonpost.com/technology/2024/01/30/parental-controls-tiktok-instagram-use/

[22] (*'Passport held by age',* ONS, available at https://www.ons.gov.uk/datasets/RM109/editions/2021/versions/1/filter-outputs/6545584b-df15-46f2-8983-a04b7e22c829)

[23] (Source: https://www.ons.gov.uk/datasets/TS007/editions/2021/versions/3)

Question	Your response
	In cases where there are false negatives and teenagers aged 14 to 16 are mistakenly identified as being under 13, approximately 75% of that age group possesses a passport. Consequently, a smaller percentage of 14 to 16-year-olds without passports or Citizen Cards would require additional support to verify their age, potentially through vouching from a professional. Yoti's white paper outlines the false positive, false negative, and true positive rates for each age range. To conclude, we would like to reiterate our disagreement with Ofcom's approach to guidance as stated in 13.75 and statements made by Ofcom's Chief Executive Officer on *Today*. We do not think that assessing children's ages is more challenging than assessing adults'. Yoti's published scientific data and the performance of FAE technology indicate otherwise. Accurate age estimation is crucial for safeguarding children online, and the current technology is adequately effective to ensure age-appropriate digital experiences. We have engaged with various Ofcom representatives, to initiate further discussions on the age threshold and broader implementation of age assurance technologies. Many stakeholders may question why Ofcom has made contradictory comments regarding the effectiveness of age assurance including facial age estimation in estimating children's ages, particularly in light of the scientific data published by Yoti and other independent audits and benchmarks. While acknowledging that no system is perfect, the current technology provides a dependable means of protecting children online. We would like to invite Ofcom and other stakeholders to engage constructively on this issue, considering the evidence presented. Prioritising online safety for children is crucial, acknowledging the capabilities of existing age assurance technologies.

Developing the Children's Safety Codes: Our framework (Section 14)	
25. Do you agree with our approach to developing the proposed measures for the Children's Safety Codes? a) If not, please explain why. 26. Do you agree with our approach and proposed changes to the draft Illegal Content Codes to further protect children and accommodate for potential synergies in how systems and processes manage both content harmful to children and illegal content? a) Please explain your views. 27. Do you agree that most measures should apply to services that are either large services or smaller services that present a medium or high level of risk to children? 28. Do you agree with our definition of 'large' and with how we apply this in our recommendations? 29. Do you agree with our definition of 'multi-risk' and with how we apply this in our recommendations? 30. Do you agree with the proposed measures that we recommend for all services, even those that are small and low-risk?	Confidential? – N We welcome the guidance set out in 14.3 '('*Services that operate across different jurisdictions have a choice: they may choose to apply all the safety protections that the Act requires for all their users, no matter where in the world; or target them specifically to users in the UK'*). We would want to see further guidance on how services would be expected to know the user's actual location, and what will happen if harm occurs to someone in the UK who accesses a service via a VPN? As we have set out in our feedback to Volume 2 ('*Identifying the services children are using Children's Access Assessments (Section 4)*'), younger Britons are more likely to use VPNs to bypass online safety measures, with high awareness among 18 to 34-year-olds, and Ofcom's research indicates that 23% of children aged 11-17 know how to use VPNs and similar workarounds. VPNs are common and low-cost, making it reasonable to expect that they will be used by children. We wonder if, similar to the recommended methodology for child assessments, where platforms must treat all users as children if they cannot determine which users are children, services should assume that all users are based in the UK unless it is clear they are not? We wonder if Ofcom will attempt to access sites using VPNs to verify whether the safety features mandated by the Online Safety Act are in place. Alternatively, is it Ofcom's policy that VPNs will nullify these measures, or will Ofcom consider encouraging age assurance at the point of entry to VPNs, if this is seen to negate age appropriate access to content? We welcome Ofcom's intention to consider responses to its previous *'Illegal Harms'* consultation. We would also like to see the same approach applied to the *'Guidance for service providers publishing pornographic content consultation'* (the *'Part 5'* service providers consultation), ensuring that principles and language are aligned across all three consultations. We would also welcome more transparency about the evidence collected by Ofcom, which is mentioned in 14.27 and 14.28. In response to the point made in 14.26 (*'Where we highlight current practices, this does not represent an endorsement of the service's approach, nor does it mean that the service is meeting the requirements of the code or an indication of compliance'*), we would encourage Ofcom in in future to provide examples of sites that would be deemed to be demonstrating '*safe harbour*', or anonymised examples of best practices. We also think it is important for Ofcom to encourage, disseminate and reward examples of best practices and providers who take extra steps to protect their users. We note the point made in 14.40 (*'Our approach is consistent with the principles of the United Nations Convention on the Rights of the Child, and in particular the provision that the best interests of the child should be a primary consideration in all regulatory actions concerning children. This is reflected in the children's safety duties and the way that the Act requires Ofcom to seek to secure a higher level of protection for children than for adults*.'). We would reinforce our feedback to Volume 3 (*'The causes and impacts of online harm to children'*), and in particular the importance of considering the risk to children in different age groups of encountering content harmful to children. Independent research and Ofcom's own research make it clear that there are

	varying levels of harm between, for instance, pre-adolescents and late-adolescents. We would also repeat the feedback provided in response to Volume 5 (*'What should services do to mitigate the risk of online harms'*), and in particular reinforce the evidence we have provided that technology is able to correctly and accurately distinguish between children of different age groups. We therefore conclude it would be in children's best interest for Ofcom to recommend that providers understand which age groups children belong to, and offer them tailored experiences. So, whilst we welcome this guidance as a step in the right direction, we do not believe it is fully consistent with the *'best interests of the child'* yet, as it incorrectly assesses that age assurance technology is not able to support providers in affording children of different age groups enhanced protection. Whilst we agree that there will be a *'higher level of protection for children than for adults'*, we think this level could be higher. We also believe that this approach would comply with the approach stated in 14.45, as a requirement to assess different age groups of children would not incur additional costs for services which will be required to implement age assurance measures anyway. Whilst we agree with the statements made in 14.64 that *'costs [are] often expected to scale with the potential benefit, in terms of reduced harm to children'*, we think that Ofcom can go further on its *'package of measures'*, especially in the field of age groups, and that this package would still be *'proportionate given its expected contribution to child safety online'*. We welcome Ofcom's approach in 14.57 to *'broadly align our approach to determining larger services with other international regimes where possible, to reduce the potential burden of regulatory compliance for services*.' We hope to see alignment and cooperation between the UK's Online Safety and the EU's Digital Services Act regimes. This work should build on the co-operation achieved via the Digital Regulation Cooperation Forum (DRCF) and the previous work of the ICO's Age Appropriate Design Code and its linkages with the European Union's Better Internet for Kids Strategy (BIK+) and Special Group on an EU Code of Conduct for age-appropriate design. We would welcome more information about when Ofcom plans to submit '*a Statement on our regulatory documents and conclusions on* our guidance Codes of Practice' (14.66). We would also like to see more information about how Ofcom would define the *'early regulatory period'* (14.68). We note Ofcom's statements at 14.69 (*'When the children's safety duties come into effect (following Codes of Practice being published), it may take time for services to bring themselves fully into compliance'*, and *'however, we expect services to take proactive steps to effectively implement safety measures as soon as is reasonably possible to protect children'*) and 14. 70 (*'all services should expect to be held to full compliance shortly after the relevant duty coming into effect'* and *'we may wish to take early action'*). Given that the success of the regime depends on robust and thorough regulatory action from Ofcom, we would like to see clear quantification of terms such as *'time'*, *'reasonably'*, *'shortly after'* and *'early action'* to ensure that service providers are incentivised to act decisively and swiftly to protect child users on their sites.
Age assurance measures (Section 15)	

31. Do you agree with our proposal to recommend the use of highly effective age assurance to support Measures AA1-6? Please provide any information or evidence to support your views. a) Are there any cases in which HEAA may not be appropriate and proportionate? b) In this case, are there alternative approaches to age assurance which would be better suited? 32. Do you agree with the scope of the services captured by AA1-6? 33. Do you have any information or evidence on different ways that services could use highly effective age assurance to meet the outcome that children are prevented from encountering identified PPC, or protected from encountering identified PC under Measures AA3 and AA4, respectively? 34. Do you have any comments on our assessment of the implications of the proposed Measures AA1-6 on children, adults or services? a) Please provide any supporting information or	Confidential? – Y (Pricing section on pg 29 marked 'TO BE REDACTED*) **Introductory statement ('*15. Age assurance measures')*** Similarly to the feedback provided above ('*Volume 4: How should services assess the risk of online harms?*'), we would suggest rephrasing 'establishing users' ages (...)' to make it clear to providers that they should limit data collection to what is necessary to determine if a user is a child so that an exact age and date of birth should not be collected unless absolutely necessary and proportional to the risk. We also welcome the aim of making *'children's experiences more age-appropriate'* and note that it is said Ofcom has *'considered the current state of technology for establishing the age of users, as well as the rapid pace of development in this industry'*. Here we would reiterate the point we have made throughout our response, but especially in our feedback to Volume 5 (*'What should services do to mitigate the risk of online harms'*). For the numerous reasons outlined in this section, we believe that Ofcom has failed to accurately assess the current state of the UK and global age assurance industry. The industry's capabilities are far more advanced than assumed in this guidance document and can significantly enhance age-appropriate experiences for children based on their age groups, beyond what Ofcom has stated. As noted by Ofcom, age assurance is *'important'* in *'ensuring that children have age-appropriate experiences online'*. ***'What is age assurance*?' section** We would provide similar feedback about 15.2 (*'establishing age'*) than to the introductory text. We support the approach taken in 15.12 to set consistent age assurance standards and requirements across both Part 3 and Part 5 providers. We welcome the approach suggested in 15.13 and would suggest that Ofcom should publish a single response document. We note the statement in 15.19 ('*While the Act recognises the need to protect children in different age groups judged to be at risk of harm from encountering PC and NDC, we are not proposing the use of age assurance to determine the specific age groups of users below the age of 18*'). Here, we would reiterate our disagreement with the approach taken as per our feedback to Volume 5 (*'What should services do to mitigate the risk of online harms'*), and our disagreement with Ofcom's assessment of the age assurance industry. We think the evidence we provide in this response presents Ofcom with an opportunity to *'adjust our recommendations on PC to focus on specific age groups'* now rather than *'in the future'*. We disagree with the suggestion that the technology needs to *'evolve'* to enable this, and would disagree that the guidance as currently set out would fully help *'offer age-appropriate experiences for children of different ages'.* We would encourage Ofcom to review the results of the ICO Sandbox undertaken ahead of the Age Appropriate Design Code in 2021 (Regulatory Sandbox Final Report: Yoti , ICO, April 2022, available at https://ico.org.uk/media/for-organisations/documents/4020427/yoti-sandbox-exit_report_20220

evidence in support of your views. 35. Do you have any information or evidence on other ways that services could consider different age groups when using age assurance to protect children in age groups judged to be at risk of harm from encountering PC?	522.pdf) and the Home Office Sandbox on Age Verification for Retail in 2022 (Age verification technology in alcohol sales, Home Office, March 2021, available sat https://www.gov.uk/government/publications/age-verification-technology-in-alcohol-sales-regulatory-sandbox and to review those results (Executive summary, Retail of Alcohol Standards Group, available at https://rasg.org.uk/wp-content/uploads/2023/11/RASG-Sandbox-Evaluation.pdf) collaboratively with scientists from across teams. We also note recent calls by a group of Members of the House of Lords who expressed their *'bewilderment'* at Ofcom's *'decision to do nothing at all to protect children under 13'*. The group also said that *'throughout the Act's passage through parliament, both HMG and Ofcom repeatedly assured us that the Act gave [Ofcom] the powers required to protect children. At no point did Ofcom raise concerns that the powers were insufficient, indeed when parliamentarians raised concerns about ensuring that age assurance was developed to create age-appropriate services, or that terms should be mandatory– we were told that 'the Children's Code would do that'*. The group also expressed its confusion *'as to why [Ofcom] has chosen not to'*. (*'Bishop Steven Calls on Ofcom to Strengthen Children's Code'*, 27 June 2024[24]. We would challenge the statement made at 15.24 (*'In our Illegal Harms Consultation, we anticipated that, where services are already using age assurance technologies, they would use these to determine whether a user is a child for these purposes'*), as there are examples of service providers who use age assurance technology to go beyond just assessing if a user is a child. Indeed, Yubo is mentioned at 15.38 (*'Yubo is a service targeted at children and young people. It uses Yoti, a third-party solution based on facial age estimation to check user age, supported by identity verification where an age estimation result requires additional checks*.'). However, it should also be made clear that Yubo utilises Yoti's age assurance to group users according to their age and provide them with an appropriate experience, including features, based on its risk assessment. Yubo utilises our facial age estimation technology and Digital ID app to age-gate its communities for 13-17 year olds and 18+. Users verify their age with a live selfie, captured within the Yubo app to prevent the use of false images. The photo is analysed in real-time by our facial age estimation AI and Yoti's liveness detection algorithm to ensure a real human is behind the camera. Users who fail these checks are asked to verify their age with an ID document. We welcome the statement made in 15.40 (*'Without age assurance, services cannot apply safety measures targeted at children in a way that ensures that all child users will benefit from an appropriately tailored experience'*), but would however caution Ofcom against using the word *'accurate'* to describe age assurance solutions based on National Insurance numbers (*'NINs'*). Indeed, NINs can be easily stolen or shared, which raises concerns about linking childrens' or adults' age assurance processes with their potentially sensitive national insurance or health information. We would like to provide feedback on the proposed age assurance methodology at 15.52. Our understanding is this will apply to providers who mainly or in part host priority content (*'PC'*) or primary priority content (*'PPC'*). Where Ofcom suggests implementing age assurance '*at a point in*

[24]https://blogs.oxford.anglican.org/bishop-steven-joins-peers-to-criticise-ofcoms-approach-to-the-childrens-code/)

	the sign-in process', we caution against the potential weakness of a one-off age assurance measure in preventing account or device sharing. Evidence from the Children's Commissioner for England's report into social media use among 8–12-year-olds found that younger children used a parent's phone to access social media services (Volume 2, *'Identifying the services children are using'*). An over-18 user could complete age verification once, and then share their account with or have it taken over by an under-18 user if the sign-in process is not robust enough. For example, if it relies solely on memorised passwords, which could easily be written down and shared, rather than biometric authentication. We recently submitted a response to a consultation by France's equivalent online safety regulator Arcom[25] on what appropriate age assurance should exist on sites that host pornographic content. In its proposal, Arcom considers that *'age verification must take place every time a service is accessed. Interrupting the session should trigger a new age verification for any subsequent access to pornographic content'*. Arcom also anticipates the issue of account or device sharing by recommending that *'in the case of a shared device between an adult and a minor, it is essential to prevent the age verification validity period from allowing access to pornographic content without a new verification'* and suggests the validity of an age check should expire *'when the session ends, the user exits the browser, or the operating system enters sleep mode'*. There is also a proposal that *'age verification should also expire after a period of one hour of inactivity'*. We would invite Ofcom to consider engaging with other regulators on the topic of token validity and expiry. We think this discussion could take place within the framework of the Global Online Safety Regulators Network (GOSRN). Still in section 15.52, we would flag that this sentence *'this means implementing age assurance at the point of entry to the site and/or ensuring that no PPC is visible to users on entering the site before they have completed an age check'* seems to contradict the previous sentence which we discuss in above in this paragraph. Indeed, implementing age assurance *'at a point in the sign-in process'* is different from implementing it *'at the point of entry to the site'*. We would invite Ofcom to make its guidance on the subject clearer and consider the proportionality of token duration and expiry. We support the statement made in 15. 53 that *'the effectiveness of an age assurance method will'*, among other things, *'depend on how it is implemented, including whether by itself or in combination with other age assurance methods'*. A point we have made throughout this response is that users should be provided with a choice of age assurance options, rather than just one, so that they may choose their preferred method or fall back on another one if they wish to challenge an age check outcome. We suggest that Ofcom could include anonymised examples of combinations of age assurance measures as examples of best practice and combinations that providers could implement as part of its guidance. We welcome the recommendations made in 15.59 that *'service providers should take steps to identify any methods children are likely to use to circumvent the age assurance methods implemented and take feasible and proportionate steps to mitigate against the use of these methods of circumvention'*. We think that Ofcom could do more

[25] (*'Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à des contenus pornographiques en ligne'*, Arcom, 11 April 2024, available at https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne)

	to support providers and the public with this recommendation, particularly by conducting and disseminating regular studies of the fraud and circumvention landscape and techniques, and through its Media Literacy and technological research workstreams. We would dispute the use of the word *'intrusive'* in 15.65 and throughout the guidance provided as a blanket word to refer to all age assurance processes and technologies. Indeed, all age assurance methods can be data minimised and not all methods require a user to provide the same amount of personal information. This unfortunate turn of phrase may lead providers to conclude, incorrectly, that age assurance is not data minimised and does not meet data protection guidelines. As we have previously stated, we believe that the risk of some players deciding to *'exit the UK market'* (15.67) can be mitigated by ensuring that Ofcom takes robust and thorough regulatory action, enforcing the regime evenly across the industry and via open collaboration with other regulators within the GOSRN. This will create a level playing field where no service provider is put at a disadvantage for implementing protective measures. This would also help reduce the risk that users have a more *'limited' 'choice of such services overall'*. We note the choice of the use of the word 'cumbersome' (15.68, 'we acknowledge that our measures will make it more cumbersome for adults to access these services'), which is defined by the Cambridge Dictionary as 'difficult to do or manage and taking a lot of time and effort'. We also note the comment in this section that 'the way services implement age assurance could in some cases dissuade adult users from using the service altogether'. We would reiterate our feedback that this will not necessarily be the case, especially if Ofcom offers providers more detailed guidance as to which measures offer less friction for users. The proposal to providers in this section to 'make their service only available to users with accounts, to reduce costs by requiring a one off age assurance check' means we would reiterate our feedback about the risk of account and device sharing, and the need for Ofcom to be clear about providers' duty to ensure that children do not access their services through device or account sharing. We understand that some users may have 'concerns about how their personal data might be used if they have to create an account on such services or how their activity may be tracked by the service'. We again believe that this can be addressed by Ofcom publishing recommendations and clear guidelines on how service providers can guarantee that no personal data is collected in this scenario, and that users will not be tracked. We also note the assessment made in 15.73 that 'all methods of age assurance will inevitably involve the processing of personal data of individuals, including children, whose personal data requires special consideration' and that '[the impact on users' privacy] will also depend on the nature of the information required to complete the highly effective age assurance process, for example, the more sensitive information required, the more intrusive the method of highly effective age assurance is likely to be'. As we have previously suggested, Ofcom could work with the ICO to ensure that there is understanding as to how data minimised age assurance meets General Data Protection Regulation (GDPR) guidance and to enhance its guidance by providing concrete examples of data minimised age assurance options which are proportionate to the use case. This would ensure that more sensitive personal information is collected only when it matches the level of risk, and that users are fully informed about this data

	processing. It should also clearly outline to providers how this data should be stored, deleted, and not used for any unintended purposes. We welcome the assessment in 15.76 that *'identity verification and age assurance are two distinct concepts'*, and that providers should be afforded *'flexibility as to the methods they use, rather than specifically recommending they should rely on identity documentation'*. In our experience platforms want to offer their consumers a choice of approaches. As we have suggested above, the concept of proportionality in age assurance methods and data collection could be linked to the potential level of risk on a platform. We support data minimised approaches *'in a way which minimises the amount of personal data which may be processed or retained, beyond what is required for implementing the age assurance process, so that it is no more than necessary'*. We reiterate our belief that providing examples of compliance and best practice could help reduce the risk that providers do not consider or fully understand these principles in their implementations. We would also note that there are data minimisation approaches which allow only an age attribute (such as 18+) to be shared through an identity verification method or a reusable digital ID app, both of which are privacy-preserving solutions. We would like to see more clarity in 15.99 (and 15.139) where for *'high risk services'*, Ofcom states that *'preventing access to the entire service using effective service-wide access controls is the only feasible solution to provide children with adequate protections from encountering PC on services in scope of this measure in practice'*. As Ofcom has previously mentioned implementing age assurance *'at a point in the sign-in process'* and '*at the point of entry'*, and given our concerns about the risk of account or device sharing (see feedback above to point 15.52), we believe it would be beneficial to clarify how age assurance is proposed to be implemented in this case. This also applies to 15.221 and the recommendation that *'services might offer users the option to unlock an unfiltered recommender feed by conducting an age check, without necessarily implementing age assurance for all users accessing the service'* In relation to 15.135, we would reiterate our previous feedback that we believe Ofcom should support service providers by conducting periodic reviews of the various age assurance solutions employed by providers in scope of the regime, conduct horizon scanning, testing, and publish the result of these alongside updating its guidance on age assurance. This is particularly important if providers are to determine *'where to position the age assurance process on their service, whether at the point of access to the service, account creation, or before a user accesses the part of the service hosting PPC'*. Such decisions should be based on an assessment of the efficacy of the age assurance measures at each described position, which could be facilitated by Ofcom. As we have stated previously, it would be useful for regulators across the GOSRN to share their knowledge in terms of the state of the art in terms of age assurance in their territories. We would like to provide feedback about the analysis of *'Costs associated with third-party age assurance methods'* (A12.25 to A12.45) provided by Ofcom in *'Annexes 10-15'*. We would challenge the approach taken in Table A12.5 (*'Illustrative cost estimates of age checks via third-party age assurance providers'*), which we believe fails to include volume discounts.

[redacted]

We would also challenge the approach taken in A12.37 (*'Costs of developing an age assurance method in-house'*), which does not consider that a service provider developing their own age assurance solution would likely also need to create an additional solution for users who fall between the age estimation buffer and the age of interest. This means that the cost of developing a solution in-house is likely to be much higher than assessed. In addition, Ofcom states in A12.37 that its thinking revolves around a consideration of *'what an age estimation method could cost to develop and run'*. However, as Ofcom's guidance acknowledges, there is a wide variety of age assurance technologies available, and the development costs would vary significantly depending on the type of technology chosen; thus, it cannot be assumed to be a single, fixed cost. We would also challenge the *'assumed overall development phase'* of *'six months'*. Audits are for instance often conducted on a 12-month cycle, and development is likely to take much longer. For instance, hiring the right personnel for development can take months, even assuming suitable candidates are immediately available. We would also challenge the assumption that there can be *'one-off labour costs relating to the upfront expense of developing, testing and deploying the so*ftware' (A12.38). Indeed, development from scratch of an age assurance approach in-house is not a one-time labour cost, it is an ongoing expense that is likely to increase over time. We would suggest that the pricing suggested in A12.40 (*'upfront staff costs could be in the region of many hundreds of thousands and potentially up to £1 million'*) and A12.41 (*'these ongoing staff costs could reach £1 million annually or potentially more'*) are indeed very conservative. In the case of AI age estimation approaches, these sections also lack a mention of the effort (including financial and legal) it would take to acquire large amounts of data to be able to accurately train a model. We would also suggest that adapting and deploying an age assurance technology in another market could take several months (for instance in terms of content localisation and local approvals) and cost considerably more than using a third-party provider. A third-party provider, already familiar with regulations and possessing ready-to-deploy solutions, offers economies of scale and efficient deployment. For instance, a solution that would have been developed in-house specifically for the UK market under the Online Safety regime could have limited portability, and therefore likely require further investment in order to be usable elsewhere.

We would like to repeat in this section the feedback we have provided above to Section 13 (Volume 5), in relation to Ofcom's decision not to have regards to the specific age groups and their exposure to harm, and the statement that it currently has *'limited independent evidence that age assurance technology can correctly distinguish between children in different age groups to a highly effective standard'*. As explained in more detail above, we believe this approach is not in

	the best interest of the child. We have pointed to the existing evidence and made that available to the regulator. (including Yoti white papers over the last 6 years, ACCS Registry of age assurance and age estimation providers, NIST Benchmarking[26] participants, AVPA directory of providers[27], KJM Raster[28]) As far back as November 2020, ACCS certified that the Yoti FAE model "can be stated to accurately estimate the age of a person of nominal age 18 as being under the age of 25 with 98.89% reliability." Yoti's September 2020 FAE model internally measured performance for 18 year olds being accurately estimated as under 25 was 99.4% based on a test sample of 7,510 individuals. For ages less than 18, as the charts show the MAE, accuracy levels increase. We would also counter the statement made in 15.318 that *'the technology for identifying the precise age of users below the age of 18 is still developing'*, again reiterating the feedback provided to Section 13. Therefore, we would express our strong disagreement that Ofcom's proposal to *'focus at this stage on establishing recommended protections for all children under the age of 18, rather tailoring those protections for children in different age groups'* should be a consequence of *'these limitations'* and believe that Ofcom's proposals as currently laid out *'are likely to have a disproportionate impact on children in different age groups'* (15.321). The technological capability clearly exists. Ofcom's statements seem to deem it immature. For instance, should additional protections be offered to the 38% of 3-4-year-olds using sites for messaging, calls, video sharing, social media, or live streaming? Should a 17-year-old be treated the same as a 7-year-old, or vice versa? We would also reiterate, in relation to the mention of *'age verification methods requiring a photo-ID document (e.g., a passport)*' which *'could identify the precise age of a user below the age of 18'*, but *'may risk excluding children from access to services they could otherwise benefit from in the absence of this documentation'*, that while service providers should be free to choose an age assurance solution they deem appropriate and proportionate to the risk of harm on their service, Ofcom could provide further guidance. Specifically, Ofcom could clarify when collecting *'the precise age of a user*' would be considered appropriate or inappropriate. There are clearly data minimised approaches available in the market, whereby via selective disclosure, only an age attribute such as over 18, 13-17, or under 18 is shared. For the many reasons specified above, we are not yet certain that the objective stated in Ofcom's guidance to provide *'sufficient clarity to services in scope of the requirements and/or our recommendations as to how they can implement age assurance in such a way that is highly effective at correctly determining whether a particular user is a child'* has yet been met. We believe that the guidance, although a big step in the right direction, could still *'lead to a material risk that providers deploy ineffective age assurance methods that do not sufficiently protect children'* in particular those in the younger age ranges 3-10 years (15.310). Nonetheless, we are confident that Ofcom can achieve this by considering our feedback and that of other industry

[26] https://pages.nist.gov/frvt/html/frvt_pad.html
[27] https://avpassociation.com/find-an-av-provider/
[28] https://www.kjm-online.de/themen/technischer-jugendmedienschutz/unzulaessige-inhalte/#c3798

	stakeholders. By bringing together a range of stakeholders to discuss the more specific issue of effective age assurance methods, they can ensure age-appropriate design for under-13-year-olds.
Content moderation U2U (Section 16)	
36. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views. 37. Do you agree with the proposed addition of Measure 4G to the Illegal Content Codes? a) Please provide any arguments and supporting evidence.	Confidential? – N Our general feedback on this section is that the effectiveness of content moderation measures implemented by service providers will depend heavily on whether they also implement robust age assurance. For this reason, it is important that Ofcom addresses the potential issues we have highlighted in our response to Section 15, such as the risk of account or device sharing, and clarifying the point(s) at which users should undergo age checks or re-authentication of age in their online journey. As Ofcom recognises (16.76), this is particularly important to support *'services that are large or multi-risk for content harmful to children'*, and which will have to implement a *'package of further steps'*.
Search moderation (Section 17)	
38. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views. 39. Are there additional steps that services take to protect children from the harms set out in the Act? a) If so, how effective are they? 40. Regarding Measure SM2, do you agree that it is proportionate to preclude users believed to be a child from turning the safe search settings off? The use of Generative AI (GenAI), see Introduction to	As an age assurance provider, Yoti is a member of civil society organisations worldwide, such as AVPA, OSTIA, FSM in Germany and Point de Contact in France. As Ofcom states that it believes *'services are generally best placed to determine how to blur content in a manner that is most effective'*, we would note that Point de Contact has recently been conducting studies on the topic of the *'blurring of search content'* (17.67), and to highlight that providers may choose different levels of blurring, some of which may still leave content visible. We believe this presents an opportunity for Ofcom's guidance in this area to be more precise or set a baseline. We are surprised by the approach taken with regards to search service in general, and in particular with the assessment that *'it would be disproportionate to recommend the use of age assurance technologies'* (17.88, a), in spite of Ofcom recognising that, as with content moderation systems, children could be exposed to 'PPC, PC, and NDC content' (17.7) in the absence of HEAA. In particular, we disagree that the only way to implement the use of age assurance technology would be *'to require every user to create an account and undergo an age check'*. (17.88, b). An age assurance process could be established independent of account creation. Like content moderation, age-restricted search results could be blocked or rendered invisible until the completion of an age check. We find it surprising that while Ofcom acknowledges in other sections of its guidance that inferring age or relying on user self-declaration are unreliable methods of age assurance, it appears to suggest these are adequate for search providers. Such methods do not meet the HEAA criteria, and we do not consider assuming *'believing the user to be a child'* to be sufficient. It is also probable that search providers will see a high level of

Volume 5, to facilitate search is an emerging development, which may include where search services have integrated GenAI into their functionalities, as well as where standalone GenAI services perform search functions. There is currently limited evidence on how the use of GenAI in search services may affect the implementation of the safety measures as set out in this code. We welcome further evidence from stakeholders on the following questions and please provider arguments and evidence to support your views: 41. Do you consider that it is technically feasible to apply the proposed code measures in respect of GenAI functionalities which are likely to perform or be integrated into search functions? 42. What additional search moderation measures might be applicable where GenAI performs or is integrated into search functions?	*'complaints about a user's access to content being restricted based on incorrect assessment of their age'* (18.18), and it is unclear in the guidance so far what search providers should do in this instance.

User reporting and complaints (Section 18)	
43. Do you agree with the proposed user reporting measures to be included in the draft Children's Safety Codes? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 44. Do you agree with our proposals to apply each of Measures UR2 (e) and UR3 (b) to all services likely to be accessed by children for all types of complaints? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response.	We would welcome more clarification on how Ofcom proposes service providers assess complaints about *'incorrect assessment of age'* (18.193), and in particular how they should assess or quantify *'the seriousness of the restriction'*. We also think there should be more clarity as to how providers could *'reverse a decision to restrict a user's access to content on the basis of an incorrect assessment of their age'*, which we would suggest should only happen after a provider has proposed one or more alternative age assurance method(s) to the user.

45. Do you agree with the inclusion of the proposed changes to Measures UR2 and UR3 in the Illegal Content Codes (Measures 5B and 5C)? a) Please provide any arguments and supporting evidence.	

Terms of service and publicly available statements (Section 19)	
46. Do you agree with the proposed Terms of Service / Publicly Available Statements measures to be included in the Children's Safety Codes? a) Please confirm which proposed measures your views relate to and provide any arguments and supporting evidence. b) If you responded to our illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 47. Can you identify any further characteristics that may improve the clarity and accessibility of terms and statements for children? 48. Do you agree with the proposed addition of Measure 6AA to the Illegal Content Codes? a) Please provide any arguments and supporting evidence.	Confidential? – N The 5Rights Foundation document Age Appropriate Presentation of Published Terms, provides useful suggestions on this topic. (https://5rightsfoundation.com/TicktoAgree-Age_appropriate_presentation_of_published_terms.pdf). Simply deploying plain English and consulting with young people would be straightforward steps to improve the clarity of terms and statements. Examples of improved privacy statements which were developed in this way to meet the AADC include that of *'King'*, with its cartoon based privacy saga ('*Privacy Saga'*, available at https://tcs.king.com/privacy-saga/level1.html, as detailed in this blog ('King's Award-Winning *'Privacy Saga Makes Terms of Service Playful'*, available at https://newsroom.activisionblizzard.com/p/king-privacy-saga-awards).
Recommender systems (Section 20)	
49. Do you agree with the proposed recommender systems measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence. b) If you responded to our illegal harms consultation and this is	Confidential? – N In response to section 20.27 (*'it is for providers to determine when to implement highly effective age assurance so long as the relevant recommender systems measures apply to all child users' recommender feeds whether logged in or out'*), we would repeat the feedback provided in our response to Section 15. In particular, we think Ofcom could provide more guidance to providers as with content moderation systems, about the effect of the positioning of age assurance on their platforms (for instance *'at a point in the sign-in process'* or *'at the point of entry to the site'*).

relevant to your response here, please signpost to the relevant parts of your prior response. 50. Are there any intervention points in the design of recommender systems that we have not considered here that could effectively prevent children from being recommended primary priority content and protect children from encountering priority and non-designated content? 51. Is there any evidence that suggests recommender systems are a risk factor associated with bullying? If so, please provide this in response to Measures RS2 and RS3 proposed in this chapter. 52. We plan to include in our RS2 and RS3, that services limit the prominence of content that we are proposing to be classified as non-designated content (NDC), namely depressive content and body image content. This is subject to our consultation on the classification of these content categories as NDC. Do you agree with this proposal? Please provide the underlying arguments and evidence of the relevance of this content to Measures RS2 and RS3. • Please provide the underlying arguments and evidence of the relevance of this content to Measures RS2 and RS3.	Our general feedback to the estimates of the cost of integrating an age assurance technology with other proposed measures presented in *'Table 20.3: Summary of direct cost'* (and corresponding sections) is that there are numerous variables to consider when assessing these numbers, making it challenging to draw definitive conclusions. The figures presented by Ofcom ('*Table 20.4: Illustrative cost of estimates of age checks via third-party age assurance providers')* may seem significant for a small company but could appear relatively minor for a larger organisation. Additionally, the cost-effectiveness could be greatly improved if a third party, such as Yoti, provided the technology. Implementation costs could range from zero to several thousand pounds. Incorporating a third-party provider would involve integrating an age assurance solution alongside a content moderation or recommender system. In this situation, the age assurance provider supplies a 'signal', and the site owner determines how to utilise this information. In response to 20.136, we would reiterate our belief that the use of HEAA should be recommended by the regulator. We welcome the introduction of a measure to *'provide children with a means of expressing negative sentiment to provide negative feedback directly to their recommender feed'* (Measure RS3), but would flag that like recommender systems, the success of this measure hinges on the service knowing the user is a child, and therefore on the use of HEAA.
User support (Section 21)	

53. Do you agree with the proposed user support measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence. b) If you responded to our Illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response.	Confidential? – N Similarly to the feedback provided in response to Section 20, we believe that the 'user support measures' described in Section 21 largely depend on the service knowing the user is a child, and therefore on the use of HEAA. We would like to reaffirm our feedback provided in response to various sections regarding the necessity for Ofcom to expand its requirements concerning children of different age groups, given the capabilities of current technology to accommodate such needs. Our belief is reinforced by the statement in 21.300 (where providers are encouraged to *'consider creating different versions of user support materials for different age groups of children, allowing children to navigate to the version that suits them best'*), demonstrating the significant benefits of categorising children into different age groups.
Search features, functionalities and user support (Section 22)	
54. Do you agree with our proposals? Please provide underlying arguments and evidence to support your views. 55. Do you have additional evidence relating to children's use of search services and the impact of search functionalities on children's behaviour? 56. Are there additional steps that you take to protect children from harms as set out in the Act? a) If so, how effective are they? As referenced in the Overview of Codes, Section 13 and Section 17, the use of GenAI to facilitate search is an emerging development and there is currently limited evidence on how the use of GenAI in search services may affect the implementation of the safety measures as set out in this section. We welcome further evidence from stakeholders on the	Confidential? – N We would highlight to Ofcom the value in considering, in conjunction with the ICO, a recent intervention by the Italian regulator AGCom. This regulator recently required age assurance and parental consent to be implemented for minors to access OpenAI in Italy. (*'Italy lays out requirements for ChatGPT's return'*, Martech, 14 April 2023, available at https://martech.org/italy-lays-out-requirements-for-chatgpts-return/

following questions and please provide arguments and evidence to support your views: 57. Do you consider that it is technically feasible to apply the proposed codes measures in respect of GenAI functionalities which are likely to perform or be integrated into search functions? Please provide arguments and evidence to support your views.	

Combined Impact Assessment (Section 23)	
58. Do you agree that our package of proposed measures is proportionate, taking into account the impact on children's safety online as well as the implications on different kinds of services?	Confidential? – N We would reiterate here the position we have developed with regards to the cost of implementing HEAA in Section 15. We welcome the statement that Ofcom's *'combined impact assessment aims to ensure that the package of proposed measures will be effective in protecting children online, without unduly affecting user rights or undermining innovation and investment in high-quality online services for UK users'* (23.3). We also welcome Ofcom's statement that *'costs should also scale with benefits'* (23.34) and that the guidance can offer *'large potential benefits in terms of reducing harm to children'* (23.35). We reiterate our belief that the success of the Online Safety regime will depend on robust and thorough regulatory action from Ofcom
Statutory tests (Section 24)	
59. Do you agree that our proposals, in particular our proposed recommendations for the draft Children's Safety Codes, are appropriate in the light of the matters to which we must have regard? a) If not, please explain why.	No comment.
Annexes **Impact Assessments (Annex A14)**	
60. In relation to our equality impact assessment, do you agree that some of our proposals would have a positive impact on certain groups? 61. In relation to our Welsh language assessment, do you agree that our proposals are	Confidential? – N **Feedback on Annex 9 ('Amendments to Illegal Content Codes of Practice for user-to- user services and search services')** We believe that the proposed amendments A5.6 (*'any written information for users comprised in the system or process should be comprehensible based on the likely reading age of the youngest person permitted to use the service without the consent of a parent or guardian'*) and A6.5 (*'the provider should ensure that the provisions included in a publicly*

likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English? a) 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.	*available statement in accordance with Recommendation 6A are (...) written to a reading age comprehensible for the youngest person permitted to use the service without the consent of a parent or guardian'*) provide further justification to our feedback on the need for Ofcom to go further in requiring providers to consider children in different age groups. Indeed, children's level of literacy can vary greatly, and information will not be presented to a 7 year old as it will be to a 17 year old. **Feedback on the 'Proposed codes at a glance' document.** We note the summary of proposed measure GA4, which requires an internal monitoring and assurance function to provide independent assurance that measures are effective. We would like to draw Ofcom's attention to the potential conflict between having an *'internal'* and *'independent' 'monitoring and assurance function'*. If providers choose to develop age assurance technologies in-house and are not required to seek third-party certification, as third-party providers like Yoti do, there is a risk that the assurance will not be genuinely independent. We would welcome further guidance on how this function can be truly independent, perhaps drawing inspiration from the Data Protection Officer role currently in place in the UK. **Feedback on Annexes 10 - 15** We would like to provide feedback on Table A12.1: Gross Annual Wages Estimates (A12.9). We would say those assessments are generally correct, however the term *'professional occupations'* is likely to cover a large number of different roles whose salary ranges are likely to differ significantly, and it is therefore difficult to comment on the accuracy of the estimate. We would also highlight that these salary estimates are typical for employees in London. While Ofcom's guidance does consider that employees could be based overseas, it does not take into account regional variations in wages within the UK. In our experience, content moderation positions, for example, are often based outside of the UK entirely, resulting in lower costs. We welcome Ofcom's recommendation that users should be *'informed about the age assurance process before completing an age check'* and that information should be set out *'clearly and accessibly'* (*'Transparency'*, A10.70 to A10.74). At A10.72, Ofcom suggests that '*it may be helpful for services to make information on the age assurance available in the form of a pop up prior to completing the age check, for example, as a smaller, new window that appears overlayed on top of the webpage, drawing the user's attention. The text could be included in this window, or the pop up could feature a button prompting users to click for more information*'. Taking into consideration usability principles, it is not ideal to open pop-ups on a desktop as they can distract users from the task at hand or be blocked by the browser, a practice that fell into disuse a long time ago. Ideally, information such as privacy policies or terms and conditions should be visible within the context of the main task, in the

	same tab. Additionally, pop-ups are ineffective on mobile phones. We are willing to provide more insider knowledge to Ofcom's team in follow-up meetings.

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