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	Veridas Digital Authentication Solutions United Kingdom Ltd

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? – Y / N 1. As a company specialising in biometric verification and age assurance solutions, we fully agree with the proposal that service providers should only conclude that children cannot normally access a service when using highly effective age assurance methods. Our biometric solutions are designed to provide exceptional accuracy in determining users' ages, ensuring that children do not access inappropriate content or services. The use of advanced technologies, such as facial recognition, guarantees superior levels of security and protection for minors online. This approach not only complies with the proposed regulations but also reinforces trust in the safety of digital services. 2. We agree with the proposed approach to the child user condition. In our experience, the interpretation of "significant number of users who are children" should be adapted to the specific context of the service and its audience. Our age assurance solutions enable service providers to accurately and continuously assess whether their user base includes a significant number of children, using biometric data and advanced analytics. By considering various factors, such as the type of content and the service's marketing practices, our systems help providers meet this condition rigorously and effectively. This holistic and contextualised assessment ensures that appropriate measures are implemented to protect underage users. 3. We support the proposed approach to the child access assessment process. Our biometric verification systems are designed to follow, if required, a two-stage process that includes determining whether children can access the service and assessing whether child user status is met. By thoroughly documenting evidence, especially when concluding that a service is not likely to be accessible to children, our systems ensure superior transparency and accounta-

Question	Your response
	bility. This framework helps service providers conduct detailed assessments and maintain regulatory compliance, thereby improving online safety for children. The ability of our solutions to perform accurate assessments and provide robust documentation facilitates regulatory compliance and effectively protects minors in the digital environment.
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 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	Confidential? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.

Question	Your response
considered as part of cumulative harm)? 9. Have you identified risks to children from GenAI content or applications on U2U or Search services? 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.	
Draft Guidance on Content Harmful to Children (Section 8)	
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	Confidential? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.

Question	Your response
b) consider not to be harmful or c) where our current proposals should be reconsidered?	
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 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?	Confidential? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.
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	Confidential? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.

Question	Your response
Profiles for Content Harmful to Children? 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 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)**	

Question	Your response
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? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.

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? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.
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.	Confidential? – Y / N 31. As a company specializing in age verification through biometric means, we recognise the importance of implementing highly effective age assurance methods to ensure regulatory compliance and protect users, especially children. Biometric methods such as facial recognition offer superior accuracy and security in age verification,

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 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?	ensuring that age restrictions are reliably and effectively enforced. This not only strengthens child protection in digital environments but also helps mitigate the risk of access to inappropriate content. a) Are there any cases in which highly effective age assurance methods might not be appropriate and proportionate? We acknowledge that in certain contexts, such as applications where accessibility is a critical factor or in environments where biometric identification may pose technical challenges, limitations in implementing these methods may arise. However, most of the time, the benefits in terms of security and regulatory compliance outweigh these considerations. b) In such cases, are there alternative approaches to age assurance that might be better suited? Alternatives such as document validation or knowledge-based verification could be considered in situations where biometrics are not viable. However, it is important to note that these methods may be less accurate and more susceptible to fraud compared to biometrics. It is true that certain forms of age assurance and biometric technology in general can carry risks; however, it is essential to note that the state of the art allows developers and companies to mitigate the majority of these risks: **1.** Quality and non-discrimination in biometric technology have made significant progress in recent years. Evaluations conducted by international bodies such as the National Institute of Standards and Technology (NIST) play a crucial role in this advancement. NIST carries out comprehensive testing and assessment of various biometric systems, establishing benchmarks and standards for accuracy and fairness. Current evaluations, standards, and certifications have been pivotal in ensuring the advancement of biometric technology. The technology has now (in fact, there are studies in this sense since 2014) surpassed human capabilities in terms of precision and exhibits fewer biases, which if any are quantifiable in opposition to human bias. This signifies a substantial leap forward in the reliability and equity of biometric technology. Anyway, regarding the bias that is commonly attributed to biometric systems, the focus must be placed in developing, training and testing phases, where the potential issues of the system may be originated at. Should these

	phases have been appropriately designed and managed, biometry has proven to ensure a better level of equality, non-discrimination and reliability than human-based analysis. Standards and guidelines in this regard could be helpful, and it shall also be taken into account the availability of databases and the capacity to create them by developers, making collaboration by state agencies and developers in these phases highly desirable. **2.** The concept of 'Privacy by Design and by Default' is of paramount importance in the context of reducing risks associated with biometric technologies. It entails the incorporation of robust privacy measures throughout the development and implementation of biometric systems. This approach dispels prevalent myths and misconceptions, ensuring user data remains secure. It could be said that the key element in a biometric recognition system is the engine to be used. Logically, from a technical perspective, more advanced engines naturally offer greater precision, reliability, and improved system accuracy. However, this choice is also critical in ensuring data protection and user privacy. Cutting-edge biometric technologies, which are now the "state of the art", are AI-based and therefore have some inherent characteristics that significantly enhance privacy and security. To shed light on this, we can categorise biometric engine models into two types: • **Biometric models based on landmarks or "Old-school" models** "Old-school" biometric engines were the most widespread until around 7 to 10 years ago, and are based on 'landmarks' or distinctive points to identify features, for instance, when recognizing a person's face. This method entails measuring various points on the biometric characteristic, such as a facial image, resulting in a mathematical vector that summarises these measurements. This is where the name bio-metrics comes from. However, this type of model may carry data protection risks, since an individual with sufficient knowledge of the system might, based on the vector generated by this biometric engine, interpret the measurements this vector is representing of the distinctive points of the subject's face (e.g. facial image: the distance between the eyes, ears, etc.) to obtain an estimation of the original image. Therefore, with this information, it might be possible to reconstruct the original image and identify the subject. Additionally, these systems were mostly standardised, which means that anyone can learn how to use them (the

	standards are public through organisations such as NIST). While standardisation promotes interoperability (as seen in fingerprint recognition systems), it also raises significant data protection concerns. • **Biometric models based on Artificial Intelligence** Leading technology companies developing state-of-the-art systems have transitioned from "old-school" models to those based on Artificial Intelligence and, particularly neural networks. In this model, the generation of the mathematical vector is more complex than simply measuring the subject's biometric distinctive points. Here, the resulting mathematical vector is dependent on the Artificial Intelligence within the biometric engine (though the system may incorporate other mathematical variables, the core components are Artificial Intelligence algorithms). Consequently, when, for example, a facial image is processed through two different biometric engines (or even two different versions of the same engine), the resulting vectors will be entirely different. As a result, in the Artificial Intelligence-based model, even the expert engineer who designed the system cannot interpret the mathematical vector to extract information from the individual who provided their data. Therefore, having the vector does not allow for the extraction of information about the individual it belongs to or their identification. Possessing such a vector does not compromise the identity of the individual. So, it is evident that the implications for the privacy and data protection of biometric data steam from the utilisation of an AI-based biometric engine. Going back to the "privacy by design and by default", the following inherent characteristics can be said regarding this resulting biometric data: • **Irreversibility:** the biometric vectors resulting from AI-based biometric models cannot be reversed to obtain the original raw data used (e.g. the exact facial image of the individual) to create this vector. In this regard, the vector is irreversible and private, which, simplifying, could be assimilated to a hash. • **Non-interoperability:** interoperability between different systems is one of the most common concerns. Nevertheless, if it was explained before that from the same original data each version of a biometric engine created a different vector, the same would be true the other way around: each

	vector can only be interpreted by the exact version of the biometric engine that created it. While this may sometimes be inconvenient from a technological point of view, it is beneficial from a data protection perspective. • **Temporality**: in any case, it is worth mentioning that a vector is only a representation of the subject's biometric characteristic for the purpose of comparison (in a specific biometric engine), and that it does not provide any further information about the subject. Other purposes (categorisation, emotion recognition,...) may need the same raw data (e.g. a facial image) but that is a different technology/system with a different purpose. • **Controlled use**: as a consequence of the above, the modern biometric vectors are data with limited usability, and they can only be effectively utilised by the individual to whom it belongs. Even in the event of potential theft, the impact on the user is minimal. The vector alone does not grant access to any system. For recognition purposes, at least two pieces of biometric data are employed for comparison, with one usually captured simultaneously (the second can be a vector if there has been a previous registration, or another piece of data captured at that moment when there is no registration). Moreover, users can only employ their vector in systems equipped with a specific biometric engine (the one used for its creation). To further enhance security, signature and encryption techniques are typically applied if the vector is delivered to the subject. This approach would ensure that even systems employing the same engine but implemented by different entities or for different purposes remain non-interoperable. • **Renewal:** it is quite common to hear that biometric data is immutable and that in case it is compromised, the greatest risk is that it cannot be changed as one would do with a password, for example. However, this is not entirely accurate. While a person's face will certainly remain the same, the interpretation of their facial features carried out by a biometric recognition system can indeed be changed. This is made possible by what was explained earlier regarding the intrinsic dependency on the version of the biometric engine used to generate a vector: a new version of this engine will produce a completely different bio-

metric vector from the one created by the old version (even if the same facial image is used), and these two vectors will not be interoperable with each other. Therefore, knowing that creating a new version of the engine is as simple as making slight modifications to certain variables, we find that renewing vectors in case of compromise is just as straightforward as changing passwords.

- **Specific use**: although some details of the characteristics mentioned above may be more related to scenarios where biometrics are used for the purpose of recognizing or identifying a person, it must be noted that this purpose is different from that of estimating the age of a person (these systems are often considered as "biometric classification"). Therefore, in addition to what has been explained regarding the privacy of the vector itself, it should be emphasised that these are different technologies, so in terms of data protection, they serve differentiated purposes, as they do not involve the same data processing or even the same technology. The ICO has recognized this differentiation.

In conclusion, 'Privacy by Design and by Default' that can be attributed to AI-based biometric models is instrumental in dispelling myths surrounding biometric technology. It safeguards user privacy by reducing the impact of data breaches, reinforcing the concept that, in practice, biometric data remains highly secure and specific to the rightful owner, further solidifying trust in biometric systems. To try to make this idea better understood, we have come up with the following video, in which during minutes 1:15 and 1:45 we explain how this vector generation works https://youtu.be/UWAAwOKs0_g?t=75.

32. Yes, we support the proposed scope of Measures AA1-6, which aim to establish robust standards for age verification in digital services, thereby ensuring a safe environment for all users, especially minors.

We would like to take the opportunity of answering this question to propose to OFCOM other solutions that can guarantee the accuracy and precision in identifying and specifying the age of the access applicant.

1. **Age verification using an identity document and a selfie photograph.**

	This solution entails requesting the user to provide a capture of their identity document along with a selfie photograph. It is akin to the process employed in sectors such as banking, insurance, mobility, telecommunications, etc. The automatic reading of the identity document is performed to extract the date of birth, thereby facilitating the straightforward calculation of the user's current age. This method of identification also allows for the retrieval of other personal information when necessary, such as the user's name, surname, and ID number. Thus, this solution may be suitable in scenarios where a comprehensive identity verification process is conducted (known in certain contexts as KYC or Know-Your-Customer). These solutions should incorporate technology to validate the authenticity of the identity document. Otherwise, a user could potentially use a fake or altered identity document with a different date of birth. Additionally, the solution should require the capture of a selfie photograph with proof of life to enable biometric comparison between the photograph printed on the identity document and the selfie. This ensures that the bearer of the identity document is indeed its legitimate holder, preventing situations where a minor may use, for example, the identity document of a parent or legal guardian. In the realm of facial biometrics, the National Institute of Standards and Technology (NIST), under the United States Department of Commerce, evaluates the quality of biometric engines globally. According to the NIST FRTE 1:1 report dated November 21, 2023, 150 biometric systems exhibit a false positive rate of 0.000001 and a false negative rate of less than 0.005, measured in the VISA category. This means that the accuracy reaches 99.9999% when comparing faces of different individuals, while only rejecting 0.5% of cases where faces of the same individual are compared, and the individual is attempting recognition by the system. Regarding the capability to perform liveness detection to prevent attackers from impersonating users, there are international standards in place for regulation. Specifically, ISO 30107 establishes the different types of presentation attacks that must be detected. In practice, leading biometric solutions in the market hold iBeta Level 1 and Level 2 certifications according to ISO 30107, ensuring secure use of certified biometric technologies. Moreover, as mentioned, this process can be used as a second step in those scenarios where the age estimation

	system based on a facial photograph provides inconclusive results. **2. Age verification for successive service accesses (authentication).** The aforementioned process allows for verifying the user's age through a complete identity verification process. However, it is essential to ensure that the user accessing the service in subsequent accesses is of legal age, through successive authentication processes. The use of passwords and devices assumes that the user authenticating through these means is who they claim to be. However, these mechanisms do not guarantee with certainty whether the authorised user is indeed accessing the service or content. For instance, a password can be stolen or simply guessed through social engineering. Therefore, it must be considered that the use of passwords does not ensure with certainty that the person accessing the service is indeed of legal age. This is a known risk and, in some cases, an assumed one, but it is also advisable to evaluate it in defining the requirements of age verification systems. According to a report published by Google, 65% of people use the same password across all or most of the services they use. Additionally, the use of some passwords is common. For example, NordPass published the 200 most common passwords worldwide, with the password "123456" being used by more than four and a half million people. When a password is compromised, it can be exposed and put up for sale on the dark web. According to a report published in 2020 by Digital Shadows, over 15 billion passwords were published on the dark web, with an average price of $15. Therefore, in cases where passwords are used as an authentication element in successive accesses, it is essential to consider the security measures that these passwords must meet, in terms of strength, renewal, custody, etc. On the other hand, to mitigate this risk, some other sectors resort to the use of biometric technologies since authentication with these technologies relies on the user performing the process rather than on user keys or passwords. In the case of accessing the service or content, it would involve basing authentication on verifying that the accessing person is the one previously verified, and thus, of legal age. The use of these biometric technologies for access involves requesting a selfie photograph from the user at the time of access and subsequently performing

	biometric comparison against the data from the registration process (described in the previous section). This new biometric capture must feature liveness detection technologies that prevent user impersonation, similar to those described earlier. Finally, as a result of the registration process described or a similar one, authentication can be carried out through the sharing of age attributes, under a proposal similar to that introduced by the European eIDAS Regulation with the digital identity wallet. In this regard, the authentication process is simplified at the time of authentication, although it would be necessary to ensure that only the registered user has access to that wallet or app from which to share their attribute. 33. As experts in biometric identity and age verification, we have observed that the effective implementation of biometric methods can significantly reduce the risk of children encountering harmful content. These methods provide an additional layer of security by ensuring that only properly verified users can access sensitive or age-restricted content. 34. Do you have any comments on our assessment of the implications of the proposed Measures AA1-6 on children, adults, or services? Please provide any supporting information or evidence in support of your views. We endorse the assessment of the implications of Measures AA1-6, as we recognise their importance in protecting minors and enhancing online safety. Proper implementation of highly effective age assurance methods not only meets regulatory requirements but also enhances user trust and promotes a safer digital environment for all. a) Please provide any supporting information or evidence in support of your views. Our studies and experience in deploying biometric verification solutions have demonstrated a significant reduction in unauthorized access to inappropriate content among minors. This underscores the effectiveness of biometric methods compared to less secure traditional approaches.

	35. As providers of biometric verification solutions, we are committed to exploring innovative ways to tailor our methods to address the specific needs of different age groups. This may include adjustments in security settings to reflect differences in maturity and discernment among various youth user groups. We would be pleased to share our datasheet to bolster our response and provide additional details on our solution's capabilities: https://veridas.com/docs/Datasheet-Age-Verification.pdf
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? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.
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 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	Confidential? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.

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?	

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?	Confidential? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.

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. 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? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.
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 relevant to your response here, please signpost to the relevant parts of your prior response.	Confidential? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.

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.	
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	Confidential? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.

to the relevant parts of your prior response.	
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 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.	Confidential? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.

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? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.
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.	Confidential? – Y / N We acknowledge that our expertise may not specifically encompass this nuanced area, and we may not be the best qualified to answer this question comprehensively. However, we are eager to engage in further discussions and would be delighted to arrange a meeting to explore age assurance methods for protecting minors or any other related topics.
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 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	Confidential? – Y / N Yes, Veridas agrees. As Welsh can be used as well as English in the written records to be inspected by Ofcom, Welsh companies will have the same opportunities and will not require extra work to provide the written comments in English

and treating Welsh no less favourably than English.	

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