# 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** | Age Check Certification Scheme |

# 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.**<br><br>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?<br><br>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?<br><br>3. Our proposed approach to the process for children's access assessments? | Yes<br><br>**Question 1 – Highly Effective Age Assurance**<br><br>The Age Check Certification Scheme (ACCS) welcomes the opportunity to respond to OFCOM's consultation on the 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 mechanisms.<br><br>ACCS strongly supports OFCOM's proposal. Ensuring that age assurance mechanisms are highly effective is crucial for protecting children from accessing inappropriate or harmful content and services.<br><br>We submit the following evidence in support of our position:<br><br>1. ISO/IEC CD1 27566-1 – Age assurance systems – Part 1: Framework – CD stage, comments and draft submitted by the UK through BSI IST 33/5/5 national mirror committee.<br>2. ACCS 1:2020 + A1:2024 – Technical requirements for age estimation technology – with Addendum 1, settting out four levels foe age estimation (Level 1 – Basic; Level 2 – Effective; Level 3 – Highly Effective; Level 4 – Strict)<br>3. IEEE 2089.1 – Standard for online age verification<br><br>The standards, public policy and our approach to independent 3rd party conformity assessment of age assurance systems; together with the research we have conducted for Ofcom and the ICO would tend to indicate that highly effective age assurance can be supported by an indicator of confidence.<br><br>The **classification accuracy of highly effective age assurance, regardless of method, should be not less than 99%.**<br><br>However, we do not think that a simple classification accuracy for age assurance is enough to be able to demonstrate that it is highly effective.<br><br>We also think the following core characteristics of the system should be established, independently tested and certified:<br><br>1. Functional characteristics:<br>a. Age assurance systems |

| Question | Your response |
| --- | --- |
| | b. Age assurance components<br>c. Data acquisition<br>d. Binding of age assurance<br>e. Data processing<br>f. Age Assurance Practice statements<br>g. Resource Utilisation<br>h. Context in use<br>i. Guidance for policy makers<br>2. Performance characteristics:<br>a. Effective age assurance<br>b. Indicators of confidence<br>c. Performance metrics<br>d. Resource utilisation<br>e. Testability<br>f. Non-repudiation<br>3. Privacy characteristics:<br>a. Privacy by design and default<br>b. Data minimisation<br>c. Avoidance of adding to Digital footprint<br>d. User awareness<br>4. Security characteristics:<br>a. Security by design and default<br>b. Resistance to presentation attack<br>c. Contraindicators<br>d. Freshness of derived credentials<br>e. Reliability and recoverability<br>f. Fail safe<br>g. Maintainability<br>5. Acceptability characteristics:<br>a. Inclusivity<br>b. User engagement<br>c. Redress<br><br>All of these are further defined in the UK's comments from the BSI mirror committee IST 33/5/5.<br><br>**Defining effective age assurance:**<br><br>In defining effective age assurance, we have posited opposing outcomes of an age assurance system:<br><br>An age assurance system that performs effectively should:<br><br>(a) cause a content provider to grant access to goods, content or services for an individual that meets the criteria for age-related eligibility (known as a true positive - TP); or |

| Question | Your response |
| --- | --- |
| | (b) cause a content provider to refuse access to goods, content or services for an individual that does not meet the criteria for age-related eligibility (known as a true negative - TN)<br><br>Whereas an age assurance system that fails to perform effectively could:<br><br>(a) cause a content provider to grant access to goods, content or services for an individual that does not meet the criteria for age-related eligibility (known as a false positive - FP); or<br><br>(b) cause a content provider to refuse access to goods, content or services for an individual that does meet the criteria for age-related eligibility (known as a false negative - FN).<br><br>This can be described in a confusion matrix:<br><br>**Predicted Age**<br><br>\| | | Positive: Over Threshold | Negative: Under Threshold \|<br>\| *Actual Age* \| Positive: Over Threshold \| True Positives (TP) \| False Negatives (FN) \|<br>\| \| Negative: Under Threshold \| False Positives (FP) \| True Negatives (TN) \|<br><br>An age assurance system that relies solely upon asserted age should be considered ineffective for the purpose of making an age-related eligibility decision, but may be considered effective for other uses of age assurance outputs that do not involve granting access to age-restricted goods, content or services (such as access to age-appropriate transparency, news, health information, product instructions or explanatory information).<br><br>As an example: Self-asserted age are circumstances when an individual is merely asked to state their own age, tick a box to agree that they are a certain age, over or under a certain age or between an age range, or to accept terms or conditions requiring them to meet an age-related eligibility criteria without that individual having to do anything else as a part of the age assurance system. |

| Question | Your response |
| --- | --- |
| | From these outputs, a classification accuracy for the age assurance system can be identified:<br><br>Classification Accuracy= (TP+TN)/(TP+TN+FP+FN)<br><br>This can include for input parameters that affect the classification accuracy, such as configuration settings.<br><br>If the classification accuracy is expressed as a percentage, then an overall picture of the likely behaviour of an age assurance system can be identified.<br><br>**Our research indicates that a classification accuracy in excess of 99% would be highly effective age assurance.**<br><br>It is important to recognise that the accuracy will continue to improve through technological advancement, but it will (in statistical terms) never reach 100%.<br><br>There are other factors that affect age assurance effectiveness and these should also be taken into account:<br><br>**Non-Repudiation**<br><br>To be highly effective, age assurance systems should be protected against repudiation. (i.e. somebody challenging or claiming that an age assurance process did not take place)<br><br>This could include mechanisms for:<br><br>(a) Digital signatures using a secure cryptographic method to ensure the authenticity and integrity of the output. The digital signature must be verifiable by the content provider to confirm that the output has not been altered since its issuance.<br><br>(b) Timestamping each age assurance output to record the exact time of issuance. This timestamp must be tamper-evident and verifiable to provide a reliable timeline of events.<br><br>(c) Immutable logs of all transactions and outputs excluding any personally identifiable information of the individual. These logs must be securely stored and protected against unauthorized modifications or deletions, ensuring a reliable audit trail. |

| Question | Your response |
| --- | --- |
| | (d) Maintaining an audit, documenting the entire process of age assurance and output generation, including user actions, system responses, and communication between the age assurance provider and the content provider.<br><br>(e) Verification protocols for the content provider to verify the authenticity and integrity of the age assurance output. These protocols should be secure and easy to use, enabling the content provider to confirm the validity of the output without additional complexity and access to personally identifiable information of the individual.<br><br>**Configuration Settings**<br><br>The configuration settings offered by an age assurance provider to a content provider should be managed and controlled in a document agreed between an age assurance provider and a content provider which should specify:<br><br>1. The availability, if any, of configuration settings for the age assurance system;<br>a. The impact of variable configuration settings on<br>b. The functional characteristics of the age assurance system<br>c. The performance characteristics of the age assurance system<br>d. The privacy characteristics of the age assurance system<br>e. The security characteristics of the age assurance system<br>f. The acceptability characteristics of the age assurance system<br>2. The responsibilities and authorities of the parties to affect the configuration settings;<br>3. The approach to configuration management planning, change control, evaluation, disposition of change, configuration status accounting, documented configuration information and configuration audit.<br><br>**Fail Safe**<br><br>An age assurance system should fail safe. |

| Question | Your response |
| --- | --- |
| | That is the age assurance output should not cause a content provider to make an incorrect age related eligibility decision as a result of a system failure.<br><br>Age assurance systems should be designed with robust fail safe mechanisms to ensure that, in the event of a system failure or malfunction then the functional, performance, privacy, security and acceptability characteristics are not compromised.<br><br>The following characteristics outline how age assurance systems should fail safely:<br><br>(a) In the event of a system failure, the age assurance system should immediately cease the collection, processing, and transmission of user data.<br><br>(b) In the event of a data acquisition failure, the age assurance system should not establish an age assurance output.<br><br>(c) In the event of a compromise to the connection between the age assurance system and the content provider, the system should not establish an age assurance output.<br><br>(d) An age assurance system should revert to the safest default settings during a failure, ensuring that no additional personal information is inadvertently exposed or collected.<br><br>(e) An age assurance system failure should be logged and subject to swift diagnosis and remediation, which may include a repetition of the age assurance process.<br><br>**Inclusivity**<br><br>The age assurance system should be designed and implemented to ensure inclusivity, providing equitable access and accurate results for all users, regardless of their demographic characteristics.<br><br>Examples of approaches that can support inclusivity include:<br><br>(a) using universal design principles, ensuring that it is accessible to individuals with diverse abilities, including those with disabilities.<br><br>(b) compliance with standards such as the Web Content Accessibility Guidelines (WCAG).<br><br>(c) supporting multiple languages to accommodate users from different linguistic backgrounds. Interfaces, instructions, and support services should be available in the predominant |

| Question | Your response |
| --- | --- |
| | languages of the contexts in which the age assurance system is intended to be used.<br><br>(d) providing alternative input methods (e.g., voice commands, screen readers) to ensure that users who cannot use traditional input devices can still complete the age assurance process.<br><br>(e) providing alternative age assurance components.<br><br>(f) ensuring that system's design and implementation is culturally appropriate and sensitive to the norms and values of different user groups. This includes the use of culturally relevant imagery, language, and examples.<br><br>(g) ensuring that age analysis are tested and validated across diverse demographic groups to prevent bias and ensure fair treatment of all users.<br><br>**User Awareness, Engagement and Transparency**<br><br>Age assurance providers and relying parties should ensure that individuals have sufficient awareness, through the publication of an age assurance practice statement or a content provider practice statement of the process of age assurance. Sufficient and meaningful information should be provided to the individual so that they can understand, in a format and language that can be reasonably expected to understand, what data will be shared between the age assurance provider and the content provider in a given context.<br><br>Where a content provider is seeking to deploy measures to prevent and detect child sexual exploitation and abuse, a content provider may determine that user awareness of the technique(s) used to achieve that objective would be counter-productive. In such cases, a content provider practice statement may exclude such technique(s) from user awareness, but they should, nevertheless, maintain a record of the processing activity, ensure compliance with UK GDPR and the Online Safety Act.<br><br>Relying parties, supported by age assurance providers, should provide educational resources to help users understand the age assurance process, their rights, and how their data will be protected. These resources should be accessible and understandable to all users. |

| Question | Your response |
| --- | --- |
| | Relying parties, supported by age assurance providers, should plan for and accommodate users with additional needs. These could include:<br><br>(a) Users with disabilities – such as individuals who are blind or have low vision who may require screen readers, magnification tools, or Braille displays to interact with the system; individuals who are deaf or hard of hearing may need visual alerts or captions for any audio prompts; or individuals with limited hand dexterity or mobility may need alternative input methods, such as voice commands, adaptive keyboards, or switch devices.<br><br>(b) Elderly users - older adults may be experiencing cognitive decline may require simplified interfaces, clear instructions, and additional time to complete tasks; they may not be familiar with modern technology may need more intuitive design and step-by-step guidance.<br><br>(c) Children and Adolescents - Younger users may need systems that facilitate parental (or responsible adult) support, consent or supervision and they may need an interface and instructions that are age-appropriate and engaging for younger users.<br><br>(d) Language Barriers - users who do not speak the system's primary language fluently may require multi-language support, including translations of the interface, instructions, and support materials.<br><br>(e) Low Literacy Users – such as individuals with low literacy levels who may need instructions and prompts written in simple, clear language or the use of icons, images, and diagrams to help convey information.<br><br>(f) Access to Technology – such as individuals who cannot afford personal devices or reliable internet access may need the age assurance system to be accessible through public access points, such as libraries or community facilities.<br><br>(g) Limited Internet Access – such as users with limited or intermittent internet connectivity may need offline capabilities or low-bandwidth solutions so the context in use needs to ensure the system is usable in areas with limited infrastructure and technological resources.<br><br>(h) Documentation Issue – some individuals may not have standard forms of identification or consistent access to |

| Question | Your response |
| --- | --- |
| | personal documents might need alternative methods of age verification.<br><br>Personnel involved in the development, implementation, and support of the age assurance system should receive training on inclusivity principles and practices to ensure they are equipped to address the needs of diverse users.<br><br>**Privacy**<br><br>Age assurance providers and relying parties should take a proactive approach that embeds privacy into the development and operation of age assurance systems from the outset and throughout their lifecycle.<br><br>The key principles include:<br><br>(a) Privacy should be proactive, not reactive. Age assurance providers and relying parties should integrate privacy considerations into the design phase of the age assurance system to anticipate and prevent privacy risks before they occur and they should conduct regular privacy impact assessments to identify and mitigate potential privacy risks.<br><br>(b) Privacy should be the default setting to ensure that personal data is automatically protected in any system or business practice and by default, no action is required by users to protect their privacy.<br><br>(c) Privacy should be embedded into the architecture of the age assurance system, ensuring it is an integral part of the system's core functionality, including incorporating strong encryption and anonymization techniques to protect personal data throughout its lifecycle.<br><br>(d) Ensuring that the data is protected throughout its entire lifecycle, from collection to processing, storage, and eventual deletion, including through secure data transmission protocols, access controls, and regular security audits.<br><br>(e) Age assurance providers and relying parties should maintain transparency about data practices, allowing users to understand how their data is used, stored, and protected, including through clarity in their respective practice statements.<br><br>(f) The configuration settings should should be established with the more privacy preserving option selected by default. |

| Question | Your response |
| --- | --- |
| | Age assurance systems should be structured so that they do not add information to an individual's digital footprint.<br><br>In particular, they should be structured so that:<br><br>(a) Age assurance providers and relying parties cannot correlate transactions performed by the same individual on different services;<br><br>(b) A third party cannot know from which age assurance provider an individual has obtained an age assurance output;<br><br>(c) Anonymisation techniques are applied immediately after an age assurance output is provided preventing tracking and identification;<br><br>(d) Appropriate use of decentralised techniques are deployed minimising the flow of personal data through central servers;<br><br>(e) Data storage is temporary and deleted immediately after an age assurance output is provided;<br><br>(f) Appropriate generation of single-use tokens that do not link back to an individual's identity.<br><br>**Security**<br><br>Age assurance providers and relying parties should take a proactive approach that embeds information security into the development and operation of age assurance systems from the outset and throughout their lifecycle. The key principles include:<br><br>(a) Security should be proactive incorporating security considerations during the initial design phase of the age assurance system to anticipate potential threats and prevent security breaches;<br><br>(b) conducting regular threat modelling and risk assessments to identify and address security vulnerabilities early in the development process and throughout the system lifecycle;<br><br>(c) designing the system architecture with security as a core component, using secure coding practices and following industry best practices for secure software development.<br><br>(d) ensuring that the system's architecture includes strong encryption methods for data at rest and in transit to protect sensitive information. |

| Question | Your response |
| --- | --- |
| | (e) implementing a multi-layered security approach, including firewalls, intrusion detection/prevention systems, and secure access controls, to protect the system at different levels, including using defence-in-depth strategies to provide multiple layers of protection against various types of system attacks.<br><br>(f) implementing continuous monitoring of the system for security threats and vulnerabilities, using automated tools and manual audits to detect and respond to potential issues promptly.<br><br>(g) developing and maintaining an incident response plan to ensure a rapid and effective response to security breaches or other security incidents.<br><br>**Redress**<br><br>Relying parties should provide means for individuals to seek redress, including taking responsibility for any interaction with the age assurance provider on behalf of the user/individual.<br><br>Age assurance providers and relying parties should enter into written agreement on which entity is responsible for complaint handling.<br><br>The user interface should provide a user-friendly and easily accessible mechanism for individuals to file complaints or report issues related to the age assurance system. This should include clear, age-appropriate instructions on how to lodge a complaint, including what information is needed and the steps involved in the process.<br><br>Relying parties should acknowledge receipt of complaints promptly, informing the individual that their issue is being reviewed and should establish and communicate a reasonable timeframe within which complaints will be addressed and resolved.<br><br>Relying parties should ensure individuals can track the status of their complaint throughout the resolution process.<br><br>Age assurance providers and relying parties should generate regular reports on complaints and redress outcomes to identify trends, improve processes, enhance system reliability and use these insights to continuously improve the age assurance system and address recurring issues. |

| Question | Your response |
|---|---|
| | **Conclusion**<br><br>ACCS supports OFCOM's 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 mechanisms. This approach is essential for safeguarding children, ensuring regulatory compliance, and maintaining a safe and trusted digital environment.<br><br>We recommend that OFCOM continues to encourage the development and adoption of advanced age assurance technologies, and supports a standardized, privacy-conscious, and inclusive approach to age verification across all digital services.<br><br>We recommend that OFCOM sets the threshold for classification accuracy to be not less than 99%.<br><br>**Question 2 – Significant Numbers of Child Users**<br><br>ACCS supports Ofcom's proposed approach to the child user condition, including the interpretation of "significant number of users who are children." This should remain a 'question of fact' and not be predetermined by metrics or fixed criteria. We agree that service providers should consider factors such as user demographics, service type, content appeal, and usage patterns to determine if children comprise a significant portion of their user base. This comprehensive assessment ensures that appropriate age assurance measures are implemented, safeguarding children effectively while maintaining compliance with regulatory requirements and fostering a secure online environment.<br><br>**Question 3 – Children's Access Assessments.**<br><br>ACCS supports Ofcom's proposed approach to children's access assessments. |
| **Volume 3: The causes and impacts of online harm to children**<br><br>**Draft Children's Register of Risk (Section 7)** | |
| **Proposed approach:**<br><br>4. Do you have any views on Ofcom's assessment of the | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |

| Question | Your response |
| --- | --- |
| causes and impacts of online harms? Please provide evidence to support your answer.<br><br>a. Do you think we have missed anything important in our analysis?<br><br>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.<br><br>6. Do you have any views on the age groups we recommended for assessing risk by age? Please provide evidence to support your answer.<br><br>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.<br><br>**Evidence gathering for future work:**<br><br>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)?<br><br>9. Have you identified risks to children from GenAI content or applications on U2U or Search services?<br><br>a) Please Provide any information about any risks identified<br><br>10. Do you have any specific evidence relevant to our assessment | |

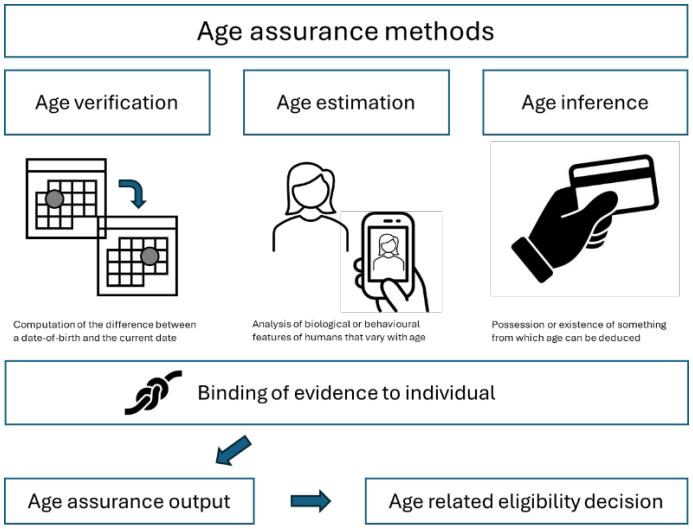
| Question | Your response |
| --- | --- |
| of body image content and depressive content as kinds of non-designated content? Specifically, we are interested in:<br>a) (i) specific examples of body image or depressive content linked to significant harms to children,<br>b. (ii) evidence distinguishing body image or depressive content from existing categories of priority or primary priority content.<br>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?<br>13. Do you have further evidence that can support the guidance provided on different kinds of content harmful to children?<br>14. For each of the harms discussed, are there additional categories of content that Ofcom<br>a) should consider to be harmful or<br>b) consider not to be harmful or<br>c) where our current proposals should be reconsidered? | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |

| Question | Your response |
|---|---|
| **Volume 4: How should services assess the risk of online harms?**<br><br>**Governance and Accountability (Section 11)** | |
| 15. Do you agree with the proposed governance measures to be included in the Children's Safety Codes?<br><br>a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence.<br>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.<br><br>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? | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |
| **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?<br><br>a) Please provide underlying arguments and evidence of efficacy or risks that support your view.<br><br>18. What do you think about our proposals in relation to the Children's Risk Profiles for Content Harmful to Children? | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |

| Question | Your response |
| --- | --- |
| a) Please provide underlying arguments and evidence of efficacy or risks that support your view.<br><br>Specifically, we welcome evidence from regulated services on the following:<br><br>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?<br><br>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?<br><br>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?<br><br>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**<br><br>**Our proposals for the Children's Safety Codes (Section 13)** | |

| Question | Your response |
| --- | --- |
| **Proposed measures**<br><br>22. Do you agree with our proposed package of measures for the first Children's Safety Codes?<br><br>a) If not, please explain why.<br><br>**Evidence gathering for future work.**<br><br>23. Do you currently employ measures or have additional evidence in the areas we have set out for future consideration?<br><br>a) If so, please provide evidence of the impact, effectiveness and cost of such measures, including any results from trialling or testing of measures.<br><br>24. Are there other areas in which we should consider potential future measures for the Children's Safety Codes?<br><br>a) If so, please explain why and provide supporting evidence. | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |

| **Developing the Children's Safety Codes: Our framework (Section 14)** | |
|---|---|
| 25. Do you agree with our approach to developing the proposed measures for the<br>Children's Safety Codes?<br>a) If not, please explain why.<br>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?<br>a) Please explain your views.<br>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?<br>28. Do you agree with our definition of 'large' and with how we apply this in our recommendations?<br>29. Do you agree with our definition of 'multi-risk' and with how we apply this in our recommendations?<br>30. Do you agree with the proposed measures that we recommend for all services, even those that are small and low-risk? | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |
| **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. | ACCS strongly supports OFCOM's proposal. Ensuring that age assurance mechanisms are highly effective is crucial for protecting children from accessing inappropriate or harmful content and services.<br>We first set out what we believe age assurance to include: |

| | |
|---|---|
| a) Are there any cases in which HEAA may not be appropriate and proportionate?<br><br>b) In this case, are there alternative approaches to age assurance which would be better suited?<br><br>32. Do you agree with the scope of the services captured by AA1-6?<br><br>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?<br><br>34. Do you have any comments on our assessment of the implications of the proposed Measures AA1-6 on children, adults or services?<br><br>a) Please provide any supporting information or evidence in support of your views.<br><br>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? |  <br><br>Age verification – is a computation process of the difference between a date-of-birth and the current date;<br><br>Age estimation – is an algorithmic analysis of biological or behavioural features of humans that vary with age (importantly this is **not** biometrics, which is associated with uniquely identifying an individual)<br><br>Age inference – is the possession or existence of something or establishing a fact from which age can be deduced<br><br>Once the method has been deployed, it can be bound to the individual and the output can be shared with the content provider to enable an age-related eligibility decision to be made.<br><br>**Evidence**<br><br>We have a considerable body of evidence to help support the development of this policy area:<br><br>In April 2024, we hosted a Global Age Assurance Standards Summit. This led to the publication of a Communique and and Compendium.<br><br>The Compendium provides a substantial body of evidence gathered from over 700 participants from governments, industry, academia, and civil society to develop international standards for age assurance. Supported by Safe Online, the British Standards Institution (BSI), and the Age Check Certification Scheme, the summit emphasized privacy-preserving, secure, and effective methods for age verification to protect children online while respecting adults' rights. The communique outlines key |

| | |
|---|---|
| | principles and a call to action for adopting these standards globally, promoting transparency, accountability, and cooperation among stakeholders.<br><br>The Communique is an important **consensus based** statement of the current state of age assurance standards. It highlights that:<br><br>***Age Assurance can be done.***<br><br>*Age Assurance can be deployed, with the right process for the right use cases, in a manner that is privacy preserving, secure, effective and efficient.*<br><br>*Age assurance can be a valuable tool amongst a range of measures deployed to protect children in the digital environment.*<br><br>*This would be assisted by securing International Standards, which are implemented and respected by providers of services that are required to make age related eligibility decisions.*<br><br>*Laws and regulations can create the legal framework with robust enforcement procedures in place to secure the protection of children from harm.*<br><br>*If deployed proportionately and effectively, Age Assurance represents an opportunity to enhance the fundamental rights of children in a digital age, in addition to protecting anonymity and the freedoms of adults to enjoy online goods, content and services*.<br><br>There is a considerable amount of activity going on that supports the deployment of age assurance for the protection of children online.<br><br>This includes the work of the UN Committee of the Rights of the Child outlined the range of rights at play for children in the digital environment in General comment No. 25 (2021) on children's rights in relation to the digital environment of March, 2 2021 (CRC/C/GC/25)<br><br>In addition, General Comment No. 20 on the implementation of the rights of the child during adolescence (CRC/C/GC/20), in which the United Nations recognized the importance of protecting children from all forms of violence, abuse and exploitation in the digital environment. |

| | |
|---|---|
| | There is the United Nations Commission on International Trade Law, Working Group IV: Electronic Commerce addressing identity and trust services [UN/A/CN.9/WG.IV].<br><br>CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.<br><br>The UN Guiding Principles (UNGPs) on Business and Human Rights set out the responsibility of companies to respect human rights and children's rights in the digital environment.<br><br>At a European level CEN/CENELEC have specified age appropriate design makes reference to the need for all age assurance systems to protect the privacy of users in accordance with applicable laws, including human rights laws.[CEN-CENELEC CWA 18016 Age Appropriate Digital Services Framework]<br><br>The EU Artificial Intelligence Act follows a product safety approach, but with the new added element of a fundamental rights impact assessment. The first EU Commission standardisation request includes obligations related to fundamental rights and data protection. Standardisation bodies such as ETSI [STF 681(TCHF) Special Task Force on Age Verification] are already moving towards harmonised global standards on AI which are underpinned by the EU AI Act and are likely to include a requirement to consider fundamental rights impacts.<br><br>Where age assurance tools are deployed that in many cases they will also be used by adults in order to determine that they are not a child (for example when accessing pornography sites, gambling sites, or when purchasing age restricted goods). The 9 core international human rights instruments apply in this context to all adult and child users.<br><br>The EU Digital Services Act (DSA) Article 28 on Online protection of minors from October, 19 2022.<br><br>The Convention on the Rights of the Child and its Optional Protocols, as well as other relevant international human rights instruments, provide the legal framework for the promotion and protection of the rights of the child in the online context all point to the need for effective age assurance. |

| | |
|---|---|
| | The International Standards Organisation through ISO/IEC JTC 1/SC 27/WG 5 is developing international standards for age assurance, most specifically:<br>● ISO/IEC WD 27566 - 1 - Age Assurance Systems - Part 1: Framework<br>● ISO/IEC WD 27566 - 2 - Age Assurance Systems – Part 2: Technical approaches and guidance for implementation<br>● ISO/IEC PWI 27566 - 3 - Age Assurance Systems - Part 3: Benchmarks for benchmarking analysis<br>The Institute of Electrical and Electronics Engineers to develop a global standard IEEE 2089.1-2024 Standard for Online Age Verification.<br><br>**Guiding Principles**<br>In order to progress the deployment of age assurance, the Summit Communique (through a consensus-based approach) created a set of guiding principles:<br><br><u>Principle 1: Age assurance should be based on the rights and best interests of the individual</u><br>Guideline 1.1: Age assurance systems should aim to protect and promote the rights and best interests of the individual in the online environment, in accordance with relevant international human rights instruments.<br>Guideline 1.2: Age assurance implementation should balance the protection and the empowerment of the individual and should not unduly restrict or limit their access to online services that are beneficial or appropriate for their age, development and well-being.<br>Guideline 1.3: Age assurance implementation should take into account the evolving capacities and the diversity of situations and needs of children of different ages, backgrounds and circumstances and should respect their views and preferences.<br><br><u>Principle 2: Age assurance systems should be based on the principle of data minimization</u><br>Guideline 2.1: Age assurance systems should only collect, process and share the minimum amount of personal data necessary and proportionate to achieve the intended |

| | |
|---|---|
| | purpose of making an age related eligibility decision thus protecting and respecting the rights and best interests of the data subject. Data should not be retained unless absolutely necessary and justified.<br><br>Guideline 2.2: Age assurance systems should use non-intrusive and privacy-preserving methods and techniques, and should avoid the onward sharing of hard identifiers, such as passports or biometrics, unless absolutely necessary, proportionate and justified.<br><br>Guideline 2.3: Age assurance systems should ensure the security, confidentiality and integrity of the personal data collected, processed and shared, and should prevent any unauthorised or unlawful access, use or disclosure.<br><br><u>Principle 3: Age assurance systems should be based on the principle of transparency and accountability</u><br><br>Guideline 3.1: Age assurance systems should provide clear, accurate, comprehensible and accessible information to the individual and where this is a child, also to their parents, guardians or caregivers about the purpose, method, scope and duration of the age assurance process, and about the rights and obligations of the parties involved.<br><br>Guideline 3.2: Age assurance systems should ensure user awareness of the methods, processes and approaches to making age related eligibility decisions in a publicly available age assurance practice statement.<br><br>Guideline 3.3: Age assurance systems should provide effective mechanisms for the user and, where this is a child, also for their parents, guardians or caregivers to access, rectify, erase or object to the personal data collected, processed or shared, where applicable for the purpose of age assurance, and to lodge a complaint or seek a remedy in case of any violation of their rights.<br><br><u>Principle 4: Age assurance should be based on the principle of cooperation and participation</u><br><br>Guideline 4.1: Age assurance systems stakeholders involved in the design, development, implementation and evaluation of the system should ensure the participation and consultation of children and their parents, guardians |

| | |
|---|---|
| | or caregivers, as well as other relevant stakeholders, such as civil society, academia, industry and technical experts.<br><br>Guideline 4.2: Age assurance stakeholders should foster cooperation and coordination among different actors and sectors, such as governments, international organisations, civil society, academia, industry and technical experts, to ensure the consistency, interoperability and effectiveness of age assurance mechanisms, standards, privacy and security.<br><br>Guideline 4.3: Age assurance stakeholders should support the development and dissemination of good practice, guidance and tools for the implementation of age assurance mechanisms and standards, and should encourage innovation and research in this field.<br><br>**Independent Conformity Assessment**<br><br>We strongly support and advocate for independent 3rd party conformity assessment of age assurance systems. Any such assessment must be carried out by UKAS (or equivalent) accredited bodies.<br><br>The Age Check Certification Scheme (ACCS) was established in 2018 and is a UKAS accredited body.<br><br>This Scheme is built on a modular approach to applicable standards and technical requirements. As a part of the Application Review Process, a Certification Officer assesses the applicable requirements for the business model of the Scheme Client. There suite of applicable requirements is constantly changing as new methodologies emerge, new standards are developed and new technical requirements are introduced.<br><br>A full comprehensive current list can be found on the Standards Section of the Scheme website, but include:<br><br>• **ACCS 0: 2021 – General Scheme Rules (covering the process of certification)**<br>• **ACCS 1: 2020 – Technical Requirements for Age Estimation Technologies**<br>• **ACCS 2: 2021 – Technical Requirements for Data Protection and Privacy** |

| | |
|---|---|
| | • ACCS 3: 2021 – Technical Requirements for Age Appropriate Design for Information Society Services<br>• ACCS 4: 2020 – Technical Requirements for Age Check Systems<br>**Proof of Age Standards Scheme**<br>The Scheme is the appointed auditor for the UK's Proof of Age Standards Scheme operated by PASSCO cic – their applicable standards include:<br>• PASS 0:2022 – Proof of Age Standards Scheme – General Principles and Definitions<br>• PASS 1:2022 – Proof of Age Standards Scheme – Requirements for Identity and Age Verification<br>• PASS 2:2020 – Proof of Age Standards Scheme – Requirements for e-IDontent/uploads/PASS-1-2022-Requirements-for-Identity-and-Age-.pdf Validation Technology<br>• PASS 3:2020 – Proof of Age Standards Scheme – Requirements for Data Protection and Privacy<br>• PASS 4:2022 – Proof of Age Standards Scheme – Requirements for Proof of Age Card Design and Construction<br>• PASS 5:2023 – Proof of Age Standards Scheme – Requirements for Digital Presentation of Proof of Age<br>**National and International Standards**<br>• BS ISO/IEC 7810:2019 – Identification cards — Physical characteristics<br>• ISO 17065:2012 – Conformity assessment – Requirements for bodies certifying products, processes and services<br>• ISO/IEC 19794-5:2011 + A2:2015 – Information technology —Biometric data interchange formats — Part 5: Face image data<br>• ISO/IEC 19795-1:2006 – Information technology —Biometric performance testing and reporting — Part 1: Principles and framework<br>• ISO 27001:2022 – Information technology — Security techniques — Information security management systems – Requirements; |

| | |
|---|---|
| | • **ISO/IEC 29100:2024 – Information technology – Security techniques – Privacy Framework;**<br>• **ISO/IEC 29101:2018 – Information technology – Security techniques – Privacy Architecture Framework;**<br>• **ISO/IEC 29109-5:2019 – Information technology —Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 Part 5: Face image data**<br>• **ISO/IEC 29115:2013 – Information technology — Security techniques — Entity Authentication Assurance Framework**<br>• **ISO/IEC 30107-1:2016 – Information technology — Biometric Presentation Attack Detection**<br>• **ISO 9001:2015 – Quality Management Systems – Requirements;**<br>• **PAS 1296:2018 – Code of Practice for Age Check Services**<br><br>ACCS have now tested more than 60 digital identity and age assurance systems, providing us with a unique overview of the quality, performance characteristics, privacy and security behaviours of the world's main providers of age assurance technology.<br><br>A full list of certified age assurance providers can be found at Registry Archive \| Age Check Certification Scheme (accscheme.com)<br><br>The wider list of digital ID service providers can be found at Registry Archive \| Age Check Certification Scheme (accscheme.com).<br><br>They provide a truly global overview of the world of age assurance.<br><br>We have recently completed an Addendum to our standards, which could be used to support definition of highly effective age assurance:<br><br>This addendum to the ACCS 1:2020 Technical Requirements for Age Estimation Technologies provides descriptions for certification levels 1 - 4. Each level signifies the degree of accuracy, reliability, and compliance with standards required for age estimation technologies as set out in ACCS 1:2020. |

| | |
|---|---|
| | This addendum provides a structured framework for understanding the certification levels of age estimation technologies, ensuring that stakeholders can make informed decisions based on the level of accuracy, privacy, and ethical standards met by each technology.<br><br>The certification levels for age estimation technologies are designed to classify and differentiate the capabilities and trustworthiness of various systems. Levels 1 to 4 represent a progression from basic to strict effectiveness for age estimation technologies.<br><br>**Level 1: Basic Compliance**<br><br>Criteria:<br><br>• Meets minimum technical requirements for age estimation accuracy.<br><br>• Basic data privacy protections in place.<br><br>• Based on sampling of not less than 30 test crew subjects<br><br>• Classification accuracy not less than 80%<br><br>• Limited user interface with minimal features.<br><br>• Suitable for low-risk applications where precise age estimation is not critical.<br><br>Description:<br><br>At Level 1, the technology provides a foundational level of age estimation accuracy. It fulfils the essential technical specifications and adheres to basic data privacy guidelines. However, its application is restricted to scenarios where the risk of incorrect age estimation is minimal.<br><br>**Level 2: Effective Compliance**<br><br>Criteria:<br><br>• Improved accuracy over Level 1, with verified performance metrics.<br><br>• Enhanced data privacy measures.<br><br>• Based on sampling of not less than 300 test crew subjects in one demongraphic group<br><br>• Classification accuracy not less than 95%<br><br>• Basic user feedback mechanisms.<br><br>• Suitable for moderate-risk applications. |

| | |
|---|---|
| | Description:<br><br>Level 2 certification signifies an advancement in accuracy and privacy compared to Level 1. The technology includes better performance metrics and enhanced user feedback features, making it suitable for applications with moderate risk where more reliable age estimation is required.<br><br>**Level 3: Highly Effective Compliance**<br><br>Criteria:<br><br>• High accuracy with validated benchmarks.<br><br>• Robust data privacy and security protocols.<br><br>• Based on sampling of not less than 300 test crew subjects in each of three skin tones and in each gender<br><br>• Classification accuracy not less than 80%<br><br>• Advanced user interface with detailed feedback options.<br><br>• Suitable for high-risk applications requiring reliable age estimation.<br><br>Description:<br><br>Technologies at Level 3 offer advanced accuracy and reliability, with stringent data privacy and security measures. The user interface is more sophisticated, providing comprehensive feedback options. This level is appropriate for high-risk applications where precise age estimation is critical.<br><br>**Level 4: Strict Compliance**<br><br>Criteria:<br><br>• Superior accuracy with extensive validation.<br><br>• Comprehensive data privacy measures, including anonymization and encryption.<br><br>• Based on sampling of not less than 3000 test crew subjects (in total) covering at least three skin tone demographics, both male and female, in at least three ambient lighting settings<br><br>• Classification accuracy not less than 99%<br><br>• User interface with extensive customization and feedback features.<br><br>• Suitable for very high-risk applications. |

| | |
|---|---|
| | Description:<br><br>Level 4 certification represents technologies with superior accuracy and comprehensive data privacy protections. These systems are validated extensively and offer customizable user interfaces, making them ideal for very high-risk applications where both accuracy and privacy are paramount.<br><br>**Application of age assurance in a global context**<br><br>Based on our extensive knowledge and experience, modern technology is capable of allowing providers of content, goods, and services on the internet to verify the ages of their consumers without jeopardizing either the providers or consumers' interests in both free speech and privacy. Age assurance can be done.<br><br>Further, the burden upon both providers of internet content, goods or services and consumers in verifying age is minimal, and reducing even further as technology evolves ever more.<br><br>There are alternatives, but these too have significant drawbacks that need to be considered, software filters on devices, when properly installed, can be a useful parental tool in regulating a minor's online activity, but in practice only provides a partial solution. They are less effective than, and not a substitute for, website-based age assurance.<br><br>**The availability of age assurance services and how they work.**<br><br>Although Content Providers may perform age assurance themselves Content Providers may, and often do, contract with third-party companies ("Third-Party Services") to perform the service for a fee. It is my understanding that under the Act and its associated rules, social media companies will be able to use Third-Party Services.<br><br>When using a Third-Party Service, a Content Provider directs the consumer to provide information directly to the Third-Party Servicer who performs the age assurance and then informs the Content Provider only of the result of the check – "pass" or "fail." It does not pass on any other information.<br><br>The Third-Party Servicer does not retain a consumer's personal information other than the date of birth, which |

| | |
|---|---|
| | can be used to respond to subsequent enquiries about that user's age.<br><br>The verification process need only be performed once per user and the verification results for any individual user may be shared with other websites, thereby minimizing the need for multiple age verification checks of the same individual, subject to effective authentication of the user on reuse.<br><br>Age assurance may be performed online from home or anywhere the user has access to the internet and can usually be completed in less than a minute.<br><br>**Cost of Age Assurance**<br><br>The leading sector requiring robust age verification was initially online gambling. As an industry with a strong return per customer, it tolerated relatively high costs per age check, perhaps as much as a dollar each. Naturally, as the Age Assurance industry grew, competition put downward pressure on pricing, and it certainly halved relatively quickly.<br><br>Alongside competitive pressures, underlying costs were also falling. The earliest age verification methods almost all relied on accessing thirdparty databases such as credit reports for which there was a substantial cost per check. The more successful providers secured volume discounts but were still facing a high fixed cost base. Naturally, providers looked for cheaper ways to deliver their services, so they looked beyond credit reports to banking and telecoms where good quality data was available at a much lower cost, or even at no variable cost at all.<br><br>As a leader of an independent conformity assessment body, I cannot speak to the specific pricing offered by individual providers, but the UK Government recently published an Impact Assessment for the Online Safety Act 2023 which estimates the cost per check to be twelve cents (converted from pence), with a caveat this cost is expected to continue to fall through innovation competition and interoperability. I am aware of some providers who offer age verification at no cost to certain sectors as part of a wider digital identity service.<br><br>**Further Details**<br><br>Age Assurance is not a new or rare technology. It is widely used by thousands of sellers and their consumers |

| | |
|---|---|
| | on a daily basis around the world in a variety of contexts such as alcohol and tobacco sales, gambling, gaming, social media and, to a growing extent around the world, accessing pornography.<br><br>Third-Party Servicers continue to grow in number and improve the age verification technology. The Age Verification Providers Association (AVPA) began in 2018 with just six members. It now has thirty members and there are at least forty providers competing in the global market.<br><br>A number of methods have been developed, initially to verify age exactly, and more recently, to estimate it with an ever-increasing degree of accuracy.<br><br>**The security of data.**<br><br>Age Assurance Providers who are members of AVPA and, thus sign up to its code of conduct, do not create new databases when conducting age checks. There are, of course, sectors such as online gambling where regulators require audit trails, but the industry's general practice is *not* to retain any personal information after an age check is completed. These audited providers do not create new databases of personal data, nor track the behavior of individuals online.<br><br>During age verification processes, Age Verification providers apply the same degree of security you would expect in financial transactions.<br><br>Specifically, age verification companies have a duty of care around the protection of personal data and demonstrate their adherence to this through various forms of certification (e.g., ISO 27001, SOC2, Cyber Essentials, BSI PAS 1296, etc.) to ensure personal data is dealt with securely.<br><br>There is now a global standard in IEEE 2089.1 and an emerging global certification process under that. There is also considerable work progressing on ISO/IEC 27566 – Age assurance systems – Framework, which will form part of global certification of age assurance systems.<br><br>Age Verification providers share with a bank or healthcare provider the same risk of attacks during these interactions with consumers, but these risks are inherent to the Internet, not unique to age verification. However, it is worth noting that there is considerably less valuable |

| | |
|---|---|
| | data, if any data at all, that would be useful to a hacker being held by Age Verification providers as opposed to that data held by banks or healthcare providers.<br><br>In addition to local laws, such as GDPR in the UK and EU, there is an industry-wide certification protocol, operated by government approved auditors, which tests providers against international standards. This not only assesses the efficacy of the age check, but also data security and privacy measures. Social Media companies governed by the Act may choose to use commercially available Age Verification providers certified by these regulatory bodies, not only to consolidate their defense against potential legal claims, but also to build consumer trust and confidence.<br><br>**Effectiveness of content filtering and other methods**<br><br>Other methods exist to advance the goal of protecting children on the internet, including parental controls and web filtering technology. The first thing to note is that multiple methods are not mutually exclusive. There is no reason why both content filtering and age verification could not be deployed either consecutively or concurrently.<br><br>There are a number of correct positive assertions about content filtering technology, but it is not a panecea to solving the problem, so we observe some of the challenges associated with content filtering. We would also draw your attention to an analysis of content filtering which can be found in a report for the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs[1].<br><br>It should also be noted that content filtering is nothing new. Software to allow for filtering of adult content (including detection of the Restricted to Adults (RTA)[2] tag) has been around for many years. There is substantial evidence (described below) that it is not having any appreciable impact on reducing the access children have to offensive sexual material. |

[1]https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf
[2] https://www.rtalabel.org/

| | |
|---|---|
| | Filtering applied in the home, on the router or on laptops, tablets, and smartphones, is generally managed by parents. We know from repeated research by OFCOM, that many parents are unaware of this technology. And those aware of it often do not know how to use it, or discover their children also know how to use it or have circumvented it some other way. And finally, those who know about it and know how to use it, must still choose to use it. "Just over a quarter of parents used content filters provided by their broadband supplier, where the filters apply to all devices using that service (27%). A much larger proportion (61%) said they were aware of this feature, showing that not all parents are adopting this potentially useful control."[3] Children can be very persuasive, and parents might release the controls to allow them to access various content. A survey of US parents by Kapersky in 2021 found just 50% used any kind of parental controls.[4]<br><br>Directions on how to circumvent parental controls are easily available on the internet. And children are succeeding at getting around parental control features.[5] Some parents describe supervising the children's internet usage as "a full-time job" [6] and that they are losing the "technological arms race over parental controls in the home."[7]<br><br>One study has found that 86% of parents support laws restricting children's access to social media.[8] Content filtering software often overblocks, preventing access to educational, informative, or harmless content. This can limit children's learning opportunities and access to useful resources, which is considered in itself to be a direct breach of a child's rights to have age-appropriate access to a digital environment. See the United Nations Committee on the Rights of a Child General Comment 25[9]. |

[3] (https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf)
[4] (https://usa.kaspersky.com/about/press-releases/2021_study-finds-50-of-parents-use-parental-control-apps)
[5] *See, e.g.*, "Tech-Savvy Kids Defeat Apple's and Others' Parental-Control Features," Wall Street Journal, December 19, 2021.
[6] *Id*.
[7] https://lifehacker.com/how-your-kids-are-outsmarting-all-your-parental-control-1848249586.
[8] *See* https://www.security.org/digital-safety/parents-react-to-social-media-legislation/.
[9] (https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation).

| | |
|---|---|
| | Filtering software is also an imperfect solution. Despite advancements, many filters fail to block all harmful content, allowing some inappropriate material to slip through and many filtering tools collect data on browsing habits. This information can be mishandled or accessed by unauthorized parties. The privacy infringement concerns raised about age verification apply also to content filtering, particularly as children reach adolescence and maturity where constant surveillance of content filtering can undermine trust between children and their guardians. Research on Internet Filtering and Adolescent Exposure to Online Sexual Material[10] concluded that caregiver's use of Internet filtering had inconsistent and practically insignificant links with young people reports of encountering online sexual material.<br><br>Filtering software can reflect the biases of its developers, resulting in the blocking of content based on cultural or ideological standards that may not align with the values of all users. Overzealous filtering can infringe on children's rights to access diverse viewpoints and information, which is essential for developing critical thinking skills and understanding the world.<br><br>The dynamic nature of the internet requires constant updates to filtering algorithms to keep up with new websites and changing content. This maintenance is resource-intensive and often lags behind the creation of new harmful content. Filtering software can cause compatibility problems with other applications and devices, leading to a frustrating user experience.<br><br>High-quality filtering software can be expensive typically in the range of £3-4 per month per license. Relying solely on content filtering software can lead to complacency among parents and guardians, who may mistakenly believe that the software provides complete protection. This can result in a lack of active engagement and communication with children about safe online behaviors.<br><br>So, although content filtering has a role to play in an overall protective approach to preventing minors from accessing sexually explicit material, it needs to form part of a response by responsible parents and guardians and |

[10] Przybylski AK, Nash V. Internet Filtering and Adolescent Exposure to Online Sexual Material. Cyberpsychol Behav Soc Netw. 2018 Jul;21(7):405-410. doi: 10.1089/cyber.2017.0466. PMID: 29995533; PMCID: PMC6101267. (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6101267/)

| | |
|---|---|
| | augmented with responsibility by adult content providers and governments to reduce and limit the options and availability of routes to access the material including age verification.<br><br>**What we've learned and what's changed in the last decade**<br><br>The age-assurance methods discussed above do not necessarily add a new step to a user's visit to a new website or app because through re-usability and interoperability, one age check can be used across multiple sites seamlessly.<br><br>The user need only complete the age-assurance process once before they can reach their subsequent objectives. For websites and apps where users create accounts, the users may only have to complete the age-assurance process one time. After that, the website or app can store that the user is old enough to access it and authenticate the user when the user presents the login credentials associated with the account. Websites and apps that do not have user accounts need not force their users to repeat age-assurance process each time the user tries to access the website or app because they can recognize when a user has previously completed an age check and rely on that check again.<br><br>Some adult content and social media companies are already using age assurance technology in some contexts. For example:<br><br>1. Aylo Inc, one of the Plaintiffs in this case, is already deploying age verification technologies in other jurisdictions, including in its home state country of Canada, as found recently by the Office of the Privacy Commissioner of Canada (https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2024/pipeda-2024-001/?wbdisable=true)<br><br>2. Meta Inc have deployed age assurance measures on Instagram using Yoti as a provider (see https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/);<br><br>3. PlayStation have deployed age assurance measures also using Yoti (https://www.playstation.com/en-gb/support/ac- |

| | |
|---|---|
| | count/age-verification-faq/#:~:text=Age%20verification%20allows%20us%20to,by%20our%20service%20provider%2C%20Yoti.)<br><br>4. Content verification is also now available on social media and adult content websites through services like VerifyMy (https://verifymy.io/).<br><br>Over the past 25 years, the age verification industry has developed a wider range of ways to verify age which offer users choice, including those who do not own or choose to use identity document-based approaches. They can choose, for example, age estimation techniques which do not require ownership or use of a document where the image is instantly deleted. Many hundreds of millions of age assurance checks are now undertaken globally each year. The cost has dropped dramatically, with reusability likely to lead to that trend continuing so there are no longer undue burdens on Web publishers due to the high costs of implementing age verification technologies. Nor would there necessarily be any significant loss of traffic resulting from the use of these technologies, except of course from children for whom the sites are unsuitable. The UK Government estimated in the Impact Assessment for legislation already approved by the House of Commons a cost per check of twelve cents and lower for high volume platforms, but noted cost may reduce further through interoperability and growing competition. The cost of that one 12 cent check may be defrayed across 100 websites before it might need to be repeated to maintain the ongoing integrity of the age verification ecosystem, and that is only if businesses determine that periodic re-validation is prudent.<br><br>Concerns about anonymity have also been addressed by developing age verification technology. The age verification sector was created specifically to enable users to access the sites they wished to access through the data minimized sharing of age. By selecting a trusted third party, even when selective disclosure from full identity document or digital identity wallet is used to prove age, the provider then only confirms “yes” or “no” when a website enquires “is this user an adult?” In Europe, users are given further reassurance by the enforcement of the General Data Protection Regulations (GDPR) but in the United States, contractual commitments to maintain secrecy and the threat of civil damages claims if that is |

| | |
|---|---|
| | not applied offer similar protection. Also, age assurance standards allow for vouching where a user with no documentary proof of age can ask a respected member of their community such as a teacher or doctor to confirm their age.<br><br>Whether or not privacy laws apply, globally AVPA members must adhere to a Code of Conduct[11] that requires privacy and data security. |
| **Content moderation U2U (Section 16)** | |
| 36. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.<br><br>37. Do you agree with the proposed addition of Measure 4G to the Illegal Content Codes?<br><br>a) Please provide any arguments and supporting evidence. | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |
| **Search moderation (Section 17)** | |
| 38. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.<br><br>39. Are there additional steps that services take to protect children from the harms set out in the Act?<br><br>a) If so, how effective are they?<br><br>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?<br><br>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 | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |

[11] https://avpassociation.com/membership/avpa-code-of-conduct/

| | |
|---|---|
| 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:<br><br>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?<br><br>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?<br><br>a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence.<br><br>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.<br><br>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? | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |

| | |
|---|---|
| a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence.<br><br>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.<br><br>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)?<br><br>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?<br><br>a) Please confirm which proposed measures your views relate to and provide any arguments and supporting evidence.<br><br>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.<br><br>47. Can you identify any further characteristics that may improve the clarity and accessibility of terms and statements for children?<br><br>48. Do you agree with the proposed addition of Measure 6AA to the Illegal Content Codes?<br><br>a) Please provide any arguments and supporting evidence. | In our view, both age assurance service providers and content service providers should establish age assurance practice statements and make these publicly available.<br><br>For age assurance service providers the practice statement should contain, as a minimum:<br><br>(a) The required outcome for the age-related eligibility decision identified (e.g. an under, over or between stated age eligibility requirements), including identifying any policy maker(s) that have established age-related eligibility requirements and the content of those requirements<br><br>(b) A description of age assurance components utilised by the age assurance system, including:<br><br>a. identifying the sources (including whether or not they are an authoritative source);<br><br>b. identifying whether or not they rely on primary or secondary credentials;<br><br>c. if used, identifying the age verification components being deployed to establish an age assurance output<br><br>d. if used, identifying the age estimation components being deployed to establish an age assurance output<br><br>e. if used, identifying the age inference components being deployed to establish an age assurance output<br><br>(c) A description of the indicators of confidence necessary to achieve from the age assurance system<br><br>(d) A description of how the system undertakes binding of the age assurance output to the correct individual<br><br>(e) A description of how the age assurance provider approaches protecting the privacy of users, including the data protection laws and obligations, which should include:<br><br>a. how the age assurance system meets the privacy characteristics set out in this document |

| | |
|---|---|
| | b. how only the minimal amount of personally identifiable information is processed for the purpose of meeting legal obligations and gaining the required indicators of confidence for age assurance to be established;<br><br>c. how personally identifiable information gathered for the purpose of age assurance is limited to that purpose and stored (this does not prevent data gathered for other purposes being used for those purposes, provided this is transparent and accountable);<br><br>d. how the age assurance provider will address the rights of individuals that are personally identifiable, including access to that data, challenging decisions made on the basis of inaccurate or incomplete data, solely automated decisions and addressing breaches in the security of that data<br><br>(f) A description of how the age assurance components adopted by the age assurance provider offer functionality appropriate to the capacity and age of a child or adult who might use the service;<br><br>(g) A description of how the age assurance system addresses the security characteristics set out in this document;<br><br>(h) A description of how the age assurance provider secures the use of the age assurance system is implemented in a manner that includes:<br><br>a. approaches that are accessible and inclusive to users with protected characteristics or additional needs<br><br>b. approaches that do not unduly restrict access of children or adults to services to which they should reasonably have access, for example, news, health and education services;<br><br>c. approaches that provide sufficient and meaningful information for a user to understand its operation, in a format and language that they can be reasonably expected to understand, including if they are a child or an adult<br><br>(i) A description of how the system, practice statement and approaches to age assurance system is subject to audit, certification and review. |

| | |
|---|---|
| | The content provider's practice statement should contain, as a minimum:<br><br>(a) The required outcome for the age-related eligibility decision identified (e.g. an under, over or between stated age eligibility requirements), including identifying any policy maker(s) that have established age-related eligibility requirements and the content of those requirements, including applicable indicators of confidence for the goods, content or services supplied by the content provider<br><br>(b) A description of age assurance providers (if any) utilized in the age assurance system, with appropriate cross-referencing to their age assurance practice statements<br><br>(c) A description of the methods used by or on behalf of the content provider to establish an age assurance output including:<br><br>a. if used, identifying the age verification components being deployed to establish an age assurance output<br><br>b. if used, identifying the age estimation components being deployed to establish an age assurance output<br><br>c. if used, identifying the age inference components being deployed to establish an age assurance output<br><br>(d) A description of how the content provider approaches protecting the privacy of users, including the data protection laws and obligations, which should include:<br><br>a. how the content provider minimises the amount of personally identifiable information it collects and stores about individuals during making age-related eligibility decisions<br><br>b. how personally identifiable information gathered for the purpose of age assurance is limited to that purpose and stored (this does not prevent data gathered for other purposes being used for those purposes, provided this is transparent and accountable);<br><br>c. how the content provider will address the rights of individuals that are personally identifiable, including access to that data, challenging decisions made on the |

| | |
|---|---|
| | basis of inaccurate or incomplete data, solely automated decisions and addressing breaches in the security of that data<br><br>(e) A description of how the age assurance methods adopted by the content provider offer functionality appropriate to the capacity and age of a child or adult who might use the service;<br><br>(f) A description of how the age assurance system addresses the security characteristics set out in this document;<br><br>(g) A description of how the content provider secures the use of the age assurance system is implemented in a manner that includes:<br><br>a. approaches that are accessible and inclusive to users with protected characteristics or additional needs<br><br>b. approaches that do not unduly restrict access of children or adults to services to which they should reasonably have access, for example, news, health and education services;<br><br>c. approaches that provide sufficient and meaningful information for a user to understand its operation, in a format and language that they can be reasonably expected to understand, including if they are a child or an adult<br><br>(h) A description of how an individual can seek redress;<br><br>(i) A description of how the system, practice statement and approaches to age assurance is subject to audit, certification and review. |
| **Recommender systems (Section 20)** | |
| 49. Do you agree with the proposed recommender systems measures to be included in the Children's Safety Codes? | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |

| | |
|---|---|
| a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.<br><br>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.<br><br>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?<br><br>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.<br><br>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.<br><br>• 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?<br><br>a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.<br><br>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 have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |
| **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.<br><br>55. Do you have additional evidence relating to children's use of search services and the impact of search functionalities on children's behaviour?<br><br>56. Are there additional steps that you take to protect children from harms as set out in the Act?<br><br>a) If so, how effective are they?<br><br>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:<br><br>57. Do you consider that it is technically feasible to apply the proposed codes measures in respect of GenAI | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |

| | |
|---|---|
| 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? | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |
| **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?<br>a) If not, please explain why. | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |
| **Annexes**<br>**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?<br>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?<br>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. | We have no specific response to these questions, but we do support the approach that Ofcom have taken to assessment of your duties in respect of the issues raised in the questions. |

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