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	ACT | The App Association

Your response

Question	Your response
Volume 2: Identifying the services children are using Children's Access Assessments (Section 4).	
Do you agree with our proposals in relation to children's access assessments, in particular the aspects below. Please provide evidence to support your view. 1. Our proposal that service providers should only conclude that children are not normally able to access a service where they are using highly effective age assurance? 2. Our proposed approach to the child user condition, including our proposed interpretation of "significant number of users who are children" and the factors that service providers consider in assessing whether the child user condition is met? 3. Our proposed approach to the process for children's access assessments?	Confidential? – **N** Age assurance and age verification that are currently available include self-declaration, hard identifiers (accessing existing databases of previously establish identification data), biometric estimation, profiling based on user behaviour, capacity testing, cross-account authentication, third-party age assurance provider (Digital identity, age tokens, B2B), account holder confirmation, and device/operating system controls. Assessing these technologies for effectiveness and impact on users' safety should consider the following factors: privacy preservation, proportionality, ease of use, impact on user experience, security, accessibility, transparency/accountability, and the level of friction. Self-declaration requires a user to enter their date of birth or check a box to certify they meet the minimum age required to use the online service. Self-declaration is easy to use and implement but offers a comparatively low level of assurance and puts responsibility directly on the child to report their age accurately. It is not a reliable tool because users can misreport their age and children may not understand the consequences of pretending to be older on their user experience. While easy for children to use and for businesses to implement, self-declaration seems only suitable for low risk and non-intrusive online services. Relying on hard identifiers means users must provide verified sources of their age, such as a copy of their ID or passport or other identifying information that can be cross-checked against official databases, e.g., in the UK this could be a national insurance number. While such hard identifiers provide a high level of age assurance (the documents in question have already been verified), they often contain more information than just a user's

Question	Your response
	age such as their name and address or sensitive data like race and gender, making this a highly privacy invasive mechanism. Additionally, most children will not have access to such documentation and most services require an additional verification by the parent to match the identification to the child. Additionally, this measure may be exclusionary to those who don't have government-issued or other official age documentation. Biometric scanning or facial recognition-based age assurance has become more accurate in recent years, but it continues to fail accurately recognise facial characteristics of both young children and people with darker skin tones. The level of age assurance thus varies from low to high confidence. While facial recognition can be implemented in privacy preserving ways, e.g., by discarding the user's image immediately after age has been estimated, most users do not understand the type of data that this tool collects, how it is used and how it may be further shared and stored. Such automated estimation often creates serious privacy risks because a person's face is highly sensitive personal information and if it is 'digitally stolen' it can impact a person's life without any good fixes. Inferring age by profiling creates all kinds of privacy risks and excessive data collection issues. Processing data to estimate a user's age consists of information a user chose to share about themselves as well as of information the online service provider infers or collects from the user's engagement with the service. Such information can include the time spent on the website or app, times of day the service is accessed, where a user is located, what interests are, who they interact with and more. Building detailed profiles of users, especially children, is highly invasive and heavily restricted by GDPR. Age inference based on profiling not only interferes with a child's right to privacy, but it also offers a low level of assurance if the data quality is poor or wholly inaccurate. Profiling also usually violates the data protection principle of data minimisation, and it is likely that an online service provider would collect more than it needs to estimate age.

Question	Your response
	Capacity testing means that a user's age is assessed based on an aptitude or capacity test, such as completing a puzzle or another task that would indicate their age or age range. While these tests are privacy and child-friendly and easy to implement for service providers, an adult could easily complete them on behalf of a child. Children's capacity does not equal age and children develop at different speeds, so capacity testing is not suitable for situations where the user's exact age is necessary because they may only suggest whether a child is above or below a certain age range. It also may be an exclusionary tool for children with lower aptitudes or developmental disabilities. When using cross-account authentication, a child can use an existing account to access a new service or product or feature (e.g., sign-in with Google or sign in with Apple). When the child enters the correct username and password for their existing account, the online service provider allows access for the new service or product to the child's user data via an API. Often it is unclear of what user data is being shared between the two providers, e.g., whether it is just the child's age or if name, location, and data are also being shared. While this method is convenient for children, the level of age assurance is unclear as the original authenticating provider determines the method and therefore the level of age assurance in this scenario. The opacity around which data is shared between providers further risks violating children's privacy rights. There are companies who provide identify confirmation and/or age assurance services. Such third parties can help online services providers by offering tokenized age checking, API solutions, or background checks or to users directly by providing digital IDs. Digital identities or credentials offer a high level of age assurance, and they can minimise personal data sharing, offering users more control over their identity. With a

Question	Your response
	digital identity, a user does not repeatedly need to submit documents for information on their age, as they have already done so once to the third-party digital identity provider. Once the digital identity is established, users can store it in a digital wallet and use it to identify themselves when signing up for other online services. Privacy risks exist nonetheless, as holding large amounts of personal information in a centralised database like a digital wallet can increase danger of fraud or commercial misuse. Business-to-business age assurance (B2B) minimises user engagement in age assurance, but the process lacks transparency and oversight. Users are often unaware a third party is part of the assurance process, making it difficult to obtain valid consent, especially from children. Adding a third party into the process also increases personal data sharing, exposing users to heightened privacy risks. Age tokens contain information exclusively related to a user's age, allowing the online service provider to confirm whether a user meets age requirements without having to collect any other personal information. The attribute provider that generates the age token determines the initial method of age assurance, so age tokens minimise data sharing, but the level of assurance depends on the method the provider chooses. The technology to generate age tokens is not yet widely available or taken up, but age assurance could evolve as age token innovation progresses. Account holder confirmation requires a service provider to get confirmation of a child's age or age range from a person that the provider knows to be an adult (e.g. a parent or caregiver). The adult can then either set up shared accounts or set up a child-specific account. All aspects of such a child-specific account, including design and content filtering, should provide for age-appropriate experiences. This method seems appropriate for younger children but for older children, it could pose risks to children's privacy (including privacy from parents). It could

Question	Your response
	also exclude children who struggle to obtain confirmation from a parent or caregiver as well as those children with parents who may not have access to hard identifiers like a government-issued ID. Parents already go through the process of providing confirmation of a child's age to the device manufacturer when setting up a new device for their child. To ease the burden on parents, it may be useful to allow device manufacturers to retain and provide that verification to covered platforms available for the device, should the developer choose to do so. This method would be easy to use and privacy preserving but the full picture is complicated by the fact that many families have either a lot of devices children may use or shared devices that people of different ages use. Using the device as source of truth is therefore also difficult. As the above demonstrates, there is currently not an ideal way to conduct age assurance in a way that is both accurate and privacy preserving and while each may have benefits there are also drawbacks that require implementation of further safeguards to protect a child's best interests. We therefore urge for flexibility in meeting age assurance requirements.
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	Confidential? – N The use of online platforms and social media have become a norm for minors for many years now, and are woven into the fabric of their lives. Through online platforms, access to the digital economy for minors has provided immense benefits, including but not limited to facilitating greater youth participation in the modern digital economy, enhancing civic engagement, providing

Question	Your response
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 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	open access to increased digital learning opportunities and after-school activities, broadening access to health care, and enabling social interaction with friends and family. The App Association also recognises the troubling trends reflected amongst children across the UK. Depression amongst minors is estimated to have drastically increased in recent years, bullying amongst minors is a persistent issue across the country, and a high majority of parents have concerns about their children's privacy and well-being. The App Association's community of small business technology developers is committed to doing its part to support children mental health, safety, and privacy. For example, the App Association has created a public resource to assist developers of software apps intended for use by minors, which makes clear that those developers must take extra consideration and care for minors' personal information and safety, and provides education to ensure that developers understand and comply with legal requirements and assisting law enforcement at all levels in protecting minors in digital environments, and other requirements; and that developers take further steps, past minimum legal requirements, to ensure they support and protect their minor customers (https://actonline.org/family-app-privacy/). Indeed, small business developers, in their own product development and in supporting their customers, routinely go far above and beyond those minimum legal requirements to support children's mental health, safety, and privacy. We urge Ofcom to acknowledge the many different ways that small businesses go far above and beyond minimum legal requirements; and that measures to protect child users are a means of market differentiation and that competitive dynamics drive innovation in the protection of minor users of technology. Small business developers also often build on online platform features to implement similar procedures. For example, app stores offer family plans to sign up and use

Question	Your response
definition of NDC under the Act at this stage? Please provide evidence to support your answer.	a platform along with providing parents optional settings for their children such as "asking to buy," rejecting or approving a purchase, monitoring content, or placing limits on screen time from the parent's device, allowing a parent a simplified process to see what their kids are doing on their devices and decide what limits they want to set for their children, ensuring that parents have meaningful notice of and control over how an app collects, uses, and discloses their children's personal information without imposing unnecessary burdens and costs on app developers. Competition amongst platforms incents their efforts to provide such tools to differentiate themselves from other platforms and attract more developers, which has produced revolutionary functionalities for safety and privacy protections as well as an equivalent experience for those with disabilities; this is a critical pro-competitive dynamic that should be highlighted by Ofcom. Noting our appreciation of the Ofcom's mandate and its goals, we emphasise that the debate about whether social media and online platforms are responsible for trends in children's mental health and general safety is far from settled. Studies have shown that life events impact children's mental health significantly more than minors' use of technology. The App Association calls on the UK government to comprehensively survey the landscape of relevant studies and data sources and to publicly present those results to inform this debate. At the same time, Ofcom should recognise the dynamic nature of online platforms and the apps they enable seamless access to, because as technology develops, the threads of causation that may be identified based on studies and data only a few years old may no longer be relevant or exist. We believe that such a clear-eyed evaluation of the evidence available, and its publication in full, will help Ofcom review the status of existing industry efforts and technologies to promote the health and safety of children and teenagers vis-à-vis their online activities, particularly with respect to their engagement in social media and other online platforms. Until the causality debate described above is well-settled, the App Association discourages (and urges Ofcom to discourage) new man-

Question	Your response
	dates behavior changes by small business digital economy innovators to address children's safety online based on assumed harms and that would use one-size-fits-all approaches, and we therefore appreciate Ofcom's measures and scaled approach proposed in this matter. The vast majority of parents have concerns about their children's digital/online safety. Given statistics surrounding children's use of online services and parents' growing concern about their children's privacy, some parents have taken more active steps to monitor their children's time online. These steps include enabling parental control settings on their children's devices to make sure they do not have access to inappropriate information and reading privacy policies that the child likely does not understand due to their age. However, research also shows that far fewer parents use parental settings on their children's devices, and that many parents knowingly let their children use general audience services without parental restrictions. With children spending a growing amount of time on online platforms and services, the resulting consent burden on parents creates challenges. Engaged parents in the modern age are expected to manage an avalanche of VPC documentation, which adds yet another onerous task for them to manage as they attempt to guide their children through complexities of the digital world, often while trying to keep up themselves. Knowing this, many creators of children-oriented websites and services have abandoned the sector or tinkered with their marketing to appear as a general audience service ostensibly patronised by non-child users and thus not subject to online children protection requirements. Such practices are widespread and often brazen, and fines assessed usually pale in comparison from the benefits accrued from ignoring the law. To help close this loophole and improve overall compliance, the App Association encourages Ofcom to allow platforms to innovate around tools and mechanisms for

Question	Your response
	app developers to utilize as they implement VPC. A potential innovation could include a mechanism to verify that a person is an adult and able to consent to an app's privacy policy on behalf of a child. Additionally, the platform can provide the consenting adult with a notification of the collection, use, or disclosure of the child's personal information. Finally, a platform may provide implementation methods that allow individual app developers to obtain verifiable parental consent from the parent based on the platform-level age verification. This type of collaborative effort between platforms and app developers would allow parents to make informed decisions about the apps their children use in an exponentially more streamlined and transparent fashion. Recognising that Ofcom is charged with developing voluntary guidance, policy recommendations, and a toolkit on safety-, health- and privacy-by-design for industry in developing digital products and services, the App Association also offers the following general recommendations: • It is vital that Ofcom reinforce for stakeholders within and outside of government that policy solutions must be predicated on a strong evidence base demonstrating direct causation of harms that the policy change would address, and not on assumptions, rare edge use cases, and/or hypotheticals. Such regulations should be technology-neutral and outcome-based. Further, future government actions to address protection of minors' mental health, safety, and privacy in the digital economy should not distort the role competition plays in spurring new and innovative means for supporting the same. • Ofcom should recognise the important role online platforms play in providing tools to small business developers to protect minors security and privacy (and to support accessibility), and condemn policy proposals that would remove incentives to innovative in providing such tools. • Ofcom should educate parents, guardians, caregivers and others on their rights related to, and

Question	Your response
	provide practical tips on, protecting the health, safety, and privacy of minors who use online platforms.
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 b) consider not to be harmful or c) where our current proposals should be reconsidered?	Confidential? – N We generally agree with Ofcom's proposed approach to the determination of content harmful to children.
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.	Confidential? – N We note that only apps that are directed towards children should have such structures for child safety. A determination of whether an app or website targets children should be based on the its subject matter (visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or

Question	Your 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?	online service is directed to children), and such a designation should require actual knowledge by the developer/operator that the app or website is collecting personal information directly from users of another website or online service directed to children (and, an app or website should not be considered to be directed towards children is (1) it does not collect personal information from any visitor prior to collecting age information; and (2) it prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part). Regular, general-use apps or services should not be required to train staff about child-specific issues, and should not be deemed directed to children solely because they refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link. In cases of services directed at children, the relevant staff should be trained to understand that they should act in the 'best interest of the child' when designing, developing, marketing, and operating an online service likely to be accessed by a child. Children should enjoy special privacy protections and the online service should provide features for parental control and restrictions.
Children's Risk Assessment Guidance and Children's Risk Profiles' (Section 12)	
17. What do you think about our proposals in relation to the Children's Risk Assessment Guidance? a) Please provide underlying arguments and evidence of efficacy or risks that support your view. 18. What do you think about our proposals in relation to the Children's Risk Profiles for Content Harmful to Children? a) Please provide underlying arguments and evidence of efficacy or risks that support your view.	Confidential? – N We note that only apps that are directed towards children should have such structures for child safety. A determination of whether an app or website targets children should be based on the its subject matter (visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children), and such a desig-

Question	Your response
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.	nation should require actual knowledge by the developer/operator that the app or website is collecting personal information directly from users of another website or online service directed to children (and, an app or website should not be considered to be directed towards children is (1) it does not collect personal information from any visitor prior to collecting age information; and (2) it prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part). Regular, general-use apps or services should not be required to train staff about child-specific issues, and should not be deemed directed to children solely because they refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link. In cases of services directed at children, the relevant staff should be trained to understand that they should act in the 'best interest of the child' when designing, developing, marketing, and operating an online service likely to be accessed by a child. Children should enjoy special privacy protections and the online service should provide features for parental control and restrictions.
Volume 5 – What should services do to mitigate the risk of online harms **Our proposals for the Children's Safety Codes (Section 13)**	
Proposed measures 22. Do you agree with our proposed package of measures for the first Children's Safety Codes? a) If not, please explain why. **Evidence gathering for future work.**	Confidential? – N We note that only apps that are directed towards children should have such structures for child safety. A determination of whether an app or website targets children should be based on the its subject matter (visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics

Question	Your response
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.	of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children), and such a designation should require actual knowledge by the developer/operator that the app or website is collecting personal information directly from users of another website or online service directed to children (and, an app or website should not be considered to be directed towards children is (1) it does not collect personal information from any visitor prior to collecting age information; and (2) it prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part). Regular, general-use apps or services should not be required to train staff about child-specific issues, and should not be deemed directed to children solely because they refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link. In cases of services directed at children, the relevant staff should be trained to understand that they should act in the 'best interest of the child' when designing, developing, marketing, and operating an online service likely to be accessed by a child. Children should enjoy special privacy protections and the online service should provide features for parental control and restrictions.

Developing the Children's Safety Codes: Our framework (Section 14)	
25. Do you agree with our approach to developing the proposed measures for the Children's Safety Codes? a) If not, please explain why. 26. Do you agree with our approach and proposed changes to the draft Illegal Content Codes to further protect children and accommodate for potential synergies in how systems and processes manage both content harmful to children and illegal content? a) Please explain your views. 27. Do you agree that most measures should apply to services that are either large services or smaller services that present a medium or high level of risk to children? 28. Do you agree with our definition of 'large' and with how we apply this in our recommendations? 29. Do you agree with our definition of 'multi-risk' and with how we apply this in our recommendations? 30. Do you agree with the proposed measures that we recommend for all services, even those that are small and low-risk?	Confidential? – N We note that only apps that are directed towards children should have such structures for child safety. A determination of whether an app or website targets children should be based on the its subject matter (visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children), and such a designation should require actual knowledge by the developer/operator that the app or website is collecting personal information directly from users of another website or online service directed to children (and, an app or website should not be considered to be directed towards children is (1) it does not collect personal information from any visitor prior to collecting age information; and (2) it prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part). Regular, general-use apps or services should not be required to train staff about child-specific issues, and should not be deemed directed to children solely because they refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link. In cases of services directed at children, the relevant staff should be trained to understand that they should act in the 'best interest of the child' when designing, developing, marketing, and operating an online service likely to be accessed by a child. Children should enjoy special privacy protections and the online service should provide features for parental control and restrictions.
Age assurance measures (Section 15)	

31. Do you agree with our proposal to recommend the use of highly effective age assurance to support Measures AA1-6? Please provide any information or evidence to support your views. a) Are there any cases in which HEAA may not be appropriate and proportionate? b) In this case, are there alternative approaches to age assurance which would be better suited? 32. Do you agree with the scope of the services captured by AA1-6? 33. Do you have any information or evidence on different ways that services could use highly effective age assurance to meet the outcome that children are prevented from encountering identified PPC, or protected from encountering identified PC under Measures AA3 and AA4, respectively? 34. Do you have any comments on our assessment of the implications of the proposed Measures AA1-6 on children, adults or services? a) Please provide any supporting information or 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?	Confidential? – Y / N Age assurance and age verification that are currently available to platforms include self-declaration, hard identifiers (accessing existing databases of previously establish identification data), biometric estimation, profiling based on user behaviour, capacity testing, cross-account authentication, third-party age assurance provider (Digital identity, age tokens, B2B), account holder confirmation, and device/operating system controls. Assessing these technologies for effectiveness and impact on users' safety should consider the following factors: privacy preservation, proportionality, ease of use, impact on user experience, security, accessibility, transparency/accountability, and the level of friction. Self-declaration requires a user to enter their date of birth or check a box to certify they meet the minimum age required to use the online service. Self-declaration is easy to use and implement but offers a comparatively low level of assurance and puts responsibility directly on the child to report their age accurately. It is not a reliable tool because users can misreport their age and children may not understand the consequences of pretending to be older on their user experience. While easy for children to use and for businesses to implement, self-declaration seems only suitable for low risk and non-intrusive online services. Relying on hard identifiers means users must provide verified sources of their age, such as a copy of their ID or passport or other identifying information that can be cross-checked against official databases, e.g., in the UK this could be a national insurance number. While such hard identifiers provide a high level of age assurance (the documents in question have already been verified), they often contain more information than just a user's age such as their name and address or sensitive data like race and gender, making this a highly privacy invasive mechanism. Additionally, most children will not have access to such documentation and most services require an additional verification by the parent to match the identification to the child. Additionally, this measure may

	be exclusionary to those who don't have government-issued or other official age documentation. Biometric scanning or facial recognition-based age assurance has become more accurate in recent years, but it continues to fail accurately recognise facial characteristics of both young children and people with darker skin tones. The level of age assurance thus varies from low to high confidence. While facial recognition can be implemented in privacy preserving ways, e.g., by discarding the user's image immediately after age has been estimated, most users do not understand the type of data that this tool collects, how it is used and how it may be further shared and stored. Such automated estimation often creates serious privacy risks because a person's face is highly sensitive personal information and if it is 'digitally stolen' it can impact a person's life without any good fixes. Inferring age by profiling creates all kinds of privacy risks and excessive data collection issues. Processing data to estimate a user's age consists of information a user chose to share about themselves as well as of information the online service provider infers or collects from the user's engagement with the service. Such information can include the time spent on the website or app, times of day the service is accessed, where a user is located, what interests are, who they interact with and more. Building detailed profiles of users, especially children, is highly invasive and heavily restricted by GDPR. Age inference based on profiling not only interferes with a child's right to privacy, but it also offers a low level of assurance if the data quality is poor or wholly inaccurate. Profiling also usually violates the data protection principle of data minimisation, and it is likely that an online service provider would collect more than it needs to estimate age. Capacity testing means that a user's age is assessed based on an aptitude or capacity test, such as completing a puzzle or another task that would indicate their age or age range. While these tests are privacy and child-friendly and easy to implement for service providers, an adult could easily complete them on behalf of a child.

	Children's capacity does not equal age and children develop at different speeds, so capacity testing is not suitable for situations where the user's exact age is necessary because they may only suggest whether a child is above or below a certain age range. It also may be an exclusionary tool for children with lower aptitudes or developmental disabilities. When using cross-account authentication, a child can use an existing account to access a new service or product or feature (e.g., sign-in with Google or sign in with Apple). When the child enters the correct username and password for their existing account, the online service provider allows access for the new service or product to the child's user data via an API. Often it is unclear of what user data is being shared between the two providers, e.g., whether it is just the child's age or if name, location, and data are also being shared. While this method is convenient for children, the level of age assurance is unclear as the original authenticating provider determines the method and therefore the level of age assurance in this scenario. The opacity around which data is shared between providers further risks violating children's privacy rights. There are companies who provide identify confirmation and/or age assurance services. Such third parties can help online services providers by offering tokenized age checking, API solutions, or background checks or to users directly by providing digital IDs. Digital identities or credentials offer a high level of age assurance, and they can minimise personal data sharing, offering users more control over their identity. With a digital identity, a user does not repeatedly need to submit documents for information on their age, as they have already done so once to the third-party digital identity provider. Once the digital identity is established, users can store it in a digital wallet and use it to identify themselves when signing up for other online services. Privacy risks exist nonetheless, as holding large amounts of personal information in a centralised database like a

	digital wallet can increase danger of fraud or commercial misuse. Business-to-business age assurance (B2B) minimises user engagement in age assurance, but the process lacks transparency and oversight. Users are often unaware a third party is part of the assurance process, making it difficult to obtain valid consent, especially from children. Adding a third party into the process also increases personal data sharing, exposing users to heightened privacy risks. Age tokens contain information exclusively related to a user's age, allowing the online service provider to confirm whether a user meets age requirements without having to collect any other personal information. The attribute provider that generates the age token determines the initial method of age assurance, so age tokens minimise data sharing, but the level of assurance depends on the method the provider chooses. The technology to generate age tokens is not yet widely available or taken up, but age assurance could evolve as age token innovation progresses. Account holder confirmation requires a service provider to get confirmation of a child's age or age range from a person that the provider knows to be an adult (e.g. a parent or caregiver). The adult can then either set up shared accounts or set up a child-specific account. All aspects of such a child-specific account, including design and content filtering, should provide for age-appropriate experiences. This method seems appropriate for younger children but for older children, it could pose risks to children's privacy (including privacy from parents). It could also exclude children who struggle to obtain confirmation from a parent or caregiver as well as those children with parents who may not have access to hard identifiers like a government-issued ID. Parents already go through the process of providing confirmation of a child's age to the device manufacturer when setting up a new device for their child. To ease the

	burden on parents, it may be useful to allow device manufacturers to retain and provide that verification to covered platforms available for the device, should the developer choose to do so. This method would be easy to use and privacy preserving but the full picture is complicated by the fact that many families have either a lot of devices children may use or shared devices that people of different ages use. Using the device as source of truth is therefore also difficult. As the above demonstrates, there is currently not an ideal way to conduct age assurance in a way that is both accurate and privacy preserving and while each may have benefits there are also drawbacks that require implementation of further safeguards to protect a child's best interests. We therefore urge for flexibility in meeting age assurance requirements.
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.	
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 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.	Confidential? – N We believe the actions services should take in response to reports or complaint are highly situation/context-specific, and that it is advisable for service providers to have a process for these situations in place and take good faith actions consistent with these policies based on actual knowledge. We appreciate Ofcom's recognition that a one-size-fits-all approach is not advisable, and for its

b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 44. Do you agree with our proposals to apply each of Measures UR2 (e) and UR3 (b) to all services likely to be accessed by children for all types of complaints? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 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.	efforts to scale measures taken under the Codes to risks presented by the scenario(s) at hand. We welcome the consideration of ACT | The App Association's views provided in response to the Illegal Harms Consultation in their entirety.

Terms of service and publicly available statements (Section 19)	
46. Do you agree with the proposed Terms of Service / Publicly Available Statements measures to be included in the Children's Safety Codes? a) Please confirm which proposed measures your views relate to and provide any arguments and supporting evidence. b) If you responded to our illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 47. Can you identify any further characteristics that may improve the clarity and accessibility of terms and statements for children? 48. Do you agree with the proposed addition of Measure 6AA to the Illegal Content Codes? a) Please provide any arguments and supporting evidence.	Confidential? – N Terms of service and public policy statements towards children must be easily accessible, easy-to-understand, concise and in intelligible language. It may also make sense to use standardised, machine-readable icons in policy statements directed at children.
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? – N While the types of data items analysed by AI and other technologies are not new, AI-driven analyses will provide greater potential utility of those data items, including in the context of preventing harm to children. There are many new uses for, and ways to analyse, data collected through apps and websites. While this raises privacy issues and questions surrounding consent to use data in a particular way (e.g., research, commercial product/service development), it also offers the potential for more powerful and granular access controls for consumers. While it is important for Ofcom to address AI-related privacy, consent, and modern technological capabilities in

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.	this consultation, requirements and obligations for online safety of children should be scalable and assure data is properly protected while also allowing the flow of information and responsible evolution of AI. Further, we generally encourage frameworks impacting AI to, consistent with our views above, also promote data access, including open access to appropriate machine-readable public data, development of a culture of securely sharing data with external partners, and explicit communication of allowable use paired with informed consent.
User support (Section 21)	
53. Do you agree with the proposed user support measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence. b) If you responded to our Illegal harms consultation and this is relevant to your response here, please signpost	

to the relevant parts of your prior response.	
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.	

Combined Impact Assessment (Section 23)	
58. Do you agree that our package of proposed measures is proportionate, taking into account the impact on children's safety online as well as the implications on different kinds of services?	Confidential? – N We generally support Ofcom's risk-based approach and refer to our comments above.
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? – N We generally share the goals of the Children's Safety Codes, and recommend including numerous detailed use cases of information society services showing what Ofcom believes is appropriate as well as inappropriate. Such an approach will make the code's guidance much more actionable to stakeholders, particularly small business innovators who do not have extensive budgets for compliance projects.
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? – N Yes, some of the proposals would have a positive impact on certain groups. The proposals are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English.

and treating Welsh no less favourably than English.	

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