Consultation response form

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

Consultation title	Guidance for service providers publishing pornographic content
Representing (delete as appropriate)	Organisation
Organisation name	Open Identity Exchange

Please note: Ofcom is a member of the Open Identity Exchange. No representative of Ofcom has been part of the production of this response. This content of this response represents the collective view of Open Identity Exchange members other than Ofcom. The response does not represent the views of Ofcom as a member of OIX.

Your response

Question	Your response
Question 1: Do you agree with our proposed guidance on scope? If not, please provide any information or evidence in support of your views, including descriptions of services or content where you consider it is unclear whether they fall within the scope of Part 5.	Confidential? – N The guidance does not address Age Assurance needs of the different communities affected by the legislation. Key communities would be: • Children • Performers • In-scope providers • Legitimate adult users It seems to me that most of the guidance is focussed on children, and we understand that this is driven by the legislation and is a good thing that their needs are considered. There is some consideration given to in-scope service providers and guidance offered to them about compliance which is also good.

Question	Your response
	However there seems to be little consideration of how compliance can be achieved in a way that minimises impact on the legitimate users of adult services and performers. We would suggest this is a risk to the successful delivery of the age assurance obligations at a national level. We would like to see explicit guidance (with an additional illustrative case study) on how in-scope service providers might deliver a compliant solution that also minimises the risk and impact for all communities involved.
Question 2: Do you have any comments on how our proposed guidance applies in respect of pornographic content created by generative-AI services within the scope of Part 5? Please provide any information or evidence in support of your views.	Confidential? – N OIX has no feedback to offer in this area
Question 3: Do you have any comments on our proposed guidance in respect of the kinds of age assurance which could be highly effective? If you consider there are other kinds of age assurance which have not been listed that you consider could fulfil the proposed criteria, please identify these with any supporting information or evidence.	Confidential? – N OIX offers the following feedback on the approach to effective age assurance: **4.15 Open Banking.** Open banking alone does not provide a user’s age. Age is not provided as part of the open banking API attributes. ID providers must: • cross match the bank accounts sort code and account number, along with self-declared name, address and date of birth, to a credit reference agency-based bank account validation service, • or use a direct proprietary bank API, where available, with the explicit agreement of bank. If using bank account login as proof of ID, the user should have to use a biometric authenticator to prove it this them as part of presenting the bank account, otherwise it’s too easy to ‘borrow’ a bank account of someone who is over 18 for ID proofing purposes. **4.18 Mobile-network operator (MNO) age checks.** The content restriction filer (CRF) alone cannot be relied upon. When accessing a site using WIFI, the age content

Question	Your response
	provider must call the MNO directly to validate the user’s age as WIFI bypassed the telcos own CRF check. Use of MNO data should also be subject to the MNO’s processes for age verification. In particular, if the named account holder of a child’s phone is a parent, the MNO’s process is likely to validate the holder as over 18. It is also easy to borrow someone else device to prove who you are in this context (e.g. a friend over 18). **4.19 Credit cards.** Re: “a payment processor sends a request to check the card is valid by the issuing bank”. The bank must be required to use biometric verification of the cardholder to ensure this is the cardholder. There are moves to tweak the EMV specification to include a response that the user is over 18 and the bank has used biometric authentication. At a minimum, this should be 3DS approval where the account holder must approve the request, to prevent under 18 using the account of others. **4.20 Digital Identity Wallets.** Wallets should not be part of this section 4 list of ‘proofing techniques’. Wallets are a way to store and reuse an age assurance proof, not a proofing technique in their own right. There are many services that are not wallet based that “enable users to verify and securely store their attributes, such as age, in a digital format.”. OIX refers to these as **Re-usable ID services.** Wallets are one example of a reusable ID. There should be a separate section in the guidance on the use of stored ID proofs from reusable IDs. The user can use any of the listed proofing techniques 4.15-4.19 and then create an account with a reusable ID provider that lets them re-assert the ID proof to many parties. In this instance, the user must be required use an appropriate authenticator to prove it is them. For example, a biometric bound to the ID as the point of ID proofing. Otherwise, reusable IDs will be passed from one user to another. What level and types of authenticators for Digital ID Wallets are acceptable? Ofcom might with to reference GPG44 which defines different quality measures for authenticators.

Question	Your response
Question 4: Do you agree that service providers should use the proposed criteria to determine whether the age assurance they implement which is highly effective at correctly determining whether or not a user is a child? Please provide any information or evidence in support of your views.	Confidential? – N **Accuracy** False Negative Rate / False Positive Rate settings need to be declared and then tuned over time. **Trust Framework** Age assurance providers should be certified to the UK Digital Identity and Attributes Trist Framework. This certification then brings risk signalling and dispute management into scope. OFCOM might want to consider if a supplemental scheme is needed to extend the trust framework to meet the needs of this use case. **Privacy** Age Assurance providers can provide a key role in giving end user the confidence their information is private through being a clearly separate brand from the adult content provider and offering techniques such pseudonymisation, ephemeral identifiers and zero knowledge proofs to allay users fears that their personal information will be shared. **Keeping Guidance up to date** Methods and standards for proofing ID and privacy management are evolving quickly. There needs to be a commitment from Ofcom to keep this guidance up to date, with a frequent review process and requirements for parties to upgrade to the latest guidance within a defined timescale. **Understanding who is approved under the regulations.** Ofcom should establish a register of approved ID providers and adult content service providers. This is important for the protection of under 18s and legitimate users.
Question 5: Do you have any information or evidence on the extent of circumvention risk affecting different age assurance methods and/or on any steps that providers might	Confidential? – N Circumvention risks for specific verification techniques are covered in our answers to Questions 3 and 4. Biometric authenticators should be used to ensure users cannot pass ID proofs onto others who are under 18.

Question	Your response
take to manage different circumvention risks for different methods?	Possession authenticators (e.g. a device) and Knowledge authenticators (e.g. passwords) can be too easily passed to users under 18. Ofcom should look at how the performance of biometric techniques are measured, how age assurance providers are assessed against these techniques and how their ongoing real-world performance is monitored and improved, specifically in relation to FPR/FNR.
Question 6: Do you agree with our proposed guidance that providers should consider accessibility and interoperability when implementing age assurance? Please provide any information or evidence in support of your views.	Confidential? – N The list of effective techniques does not give options to some of the ID Challenged: those who do not have access to online banking, photo ID documents or a mobile phone. **Accessibility** The regulations must ensure those who do not pass ‘challenge 25’ have access to enough alternative methods to prove who they are. Current verification methods need to be expanded to be more inclusive as it constrained to: those who have a access to online banking, photo ID documents or a mobile phone. I order to achieve 4.35.b, the wording around 4.37.b is currently too weak. A stronger statement than ‘considering’ is required in 4.37b. The guidance can offer examples of how to achieve this, such as: age restricted content providers can achieve this by going through a orchestrator or scheme that allows access to multiple alternative age assurance methods. **Interoperability** To explain interoperability better to age restricted content providers more clearly, the UX benefits for their customers should be expanded upon; from an end users’ perspective, proof of age is ideally able to be leveraged across many providers, so if a user already has a proof of age, it is accepted seamlessly as the move from site to site. Age restricted content providers should therefore seek age assurance providers, schemes or orchestrators that enable interoperability across sites. Portability of age assurance from one age assurance provider to another should be a requirement.

Question	Your response
	Figure 4.4 Step 5. Ongoing monitoring - would benefit from guidance as to how a service provider does this.
Question 7: Do you have comments on the illustrative case study we have set out in the guidance? Do you have any supporting information or evidence relating to additional examples of how the criteria and principles might apply to different age assurance processes?	Confidential? – N OIX has no feedback to offer in this area
Question 8: Do you agree with our proposed guidance on the record-keeping duties? Please provide any information or evidence in support of your views.	Confidential? – N There is no requirement for the service provider or the age assurance provider to keep transactional records of proof of age. On the flip side, nor does it say that transactional records should not be kept. Is this a consciously selected position? OIX would have expected the regulation to require parties to record transactional records of age assurance in a privacy protecting way (such as via pseudonymisation, ephemeral identifiers or zero knowledge proofs). The UK Digital Identity and Attributes trust framework requires transactional level record keeping, so if this leveraged to deliver age assurance, transactional record keeping would be introduced by default, unless Ofcom overrides that requirement, with OfDIAs agreement, through a Supplemental Scheme. We would suggest session 5.25 of the guidance is extended to reference record keeping requirements within the DIATF once this is finalised.
Question 9: Do you have any comments on our proposed approach to assessing compliance with the duties on service providers who publish or	Confidential? – N OIX has no feedback to offer in this area

Question	Your response
display pornographic content, including on the proposed examples of non-compliance? Please provide any information or evidence in support of your views.	
Question 10: Do you have any comments on the impact assessment set out in Annex 1? Please provide any information or evidence in support of your views	Confidential? – N OIX has no feedback to offer in this area
Question 11: Do you agree that our proposed guidance is likely to have positive effects on opportunities to use Welsh and treating Welsh no less favourably than English? If you disagree, please explain why, including how you consider the proposed guidance could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.	Confidential? – N OIX has no feedback to offer in this area

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