Consultation response form

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 OpenID Foundation has no feedback regarding this question
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 The OpenID Foundation has no feedback regarding this question
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 The OpenID Foundation would suggest that several of the suggested “kinds of age assurance” are in fact cases of re-usable digital identity and it would be appropriate to have “re-usable digital identity” as a general kind in this list with things like “MNO age checks,” “bank account age checks” or “digital identity wallets” “or government-issued digital identity credentials” as examples. It would also seem appropriate to have a clearly defined subset of the age assurance duties that re-usable digital

Question	Your response
	ID providers would need to perform in order for them to be used by service providers in that way.
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 There appears to be a lack of clarity (or gap) about when in a sequence of events it is expected a service provider will perform the processes related to its age assurance duties, potentially based on the assumption that there is always a 1:1 relationship between device or app and user. This observation is really about whether the age assurance duties are performed once only and then persisted for a significant period. A wide range of interpretations of that can be made from per-image to persistence over many months. This means that there may well be significant challenges for implementers in determining whether they are implementing something that puts themselves at risk of non-compliance.
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 take to manage different circumvention risks for different methods?	Confidential? – N The OpenID Foundation does not have any evidence of the extent of circumvention risk affecting different age assurance methods. However, we can speak to some of the risks and possible mitigations. In Open Banking, the banking app may not be restricted to a single biometric or fingerprint for authentication. If an adult event allowed a minor access to their bank account online then the adult's device could be used to authorise an age verification transaction via Open Banking. Or a youth might "shoulder surf to observe a PIN" and then steal the device. A mitigation is to enable biometric-binding to the device and a block on use of PIN to authenticate the transaction. In photo-ID matching, there are many ways to defraud a solution, so several steps must be in place to have confidence that the credential is a legitimate credential, and the carbon person holding the credential is the owner of the that legitimate credential. A minor may

Question	Your response
	well attempt to use a fake ID, or try to deceive the algorithm by other means (make-up, masks, AI fakes, or "failing" out of this step intentionally). Photo-ID matching can be enhanced if there is a check back to a government system of record, a check back to a government-issued identity credential held in a secure wallet on the user's device, or the photo ID matching is layered with other steps. ISO 30107 PAD Certification is recommended as one tool for conformance to a high quality technical solution. Facial age estimation. This works by analysing the features of a user's face to estimate their age. This is still a relatively new technology…so further work maybe required to ensure services provided have consistently high quality and tests to ensure conformance to a set of standards. Mobile network operator (MNO) age checks. A mobile network operator age check could be circumvented relatively easily unless there is a mechanism for biometric binding and ensuring a PIN cannot be used to unlock the device. It is also possible that a device could be "sold" or the PIN "shoulder surfed" and device stolen with the CRF of another person unless there is binding between the original age verification, and the subsequent request for access. The incentive for minors to exploit any gaps will be high to gain access to adult content, even if this is not a common problem observed at scale today. Credit card checks. An adult may give access to a minor to a credit card, and the adult may or may not intend for that card information to be saved in such a way it can later be used for access sites with restricted content. On many devices, access to content like cards is defaulted into the device or browser the user is using. The probability that the card and card account holder is an adult may be quite high in most transactions today. However, the since there would not be a payment transaction showing the age verification check on an adult's credit card statement, there would be no evidence to note the misuse by the adult, so the ease of use and incentive for minors to misuse credit cards to

Question	Your response
	access content will be high, even if this is not a common problem observed at scale today. Digital Identity Wallets are one of the most nascent technologies, but arguably one of the most promising for ensuring high confidence of identity of the user presenting a credential, and to protect user privacy. Provided that the digital credentials held in the wallet have gone through a rigorous process, then repeat presentation by the user with biometric checks and binding can be achieve in a convenient and privacy preserving way. This is similar to Apple Pay or Google Pay transactions online, but with biometric binding that ensures the person that set-up the credential is the only one that can release it. Provided the relying party only asks for what they need for compliance to access a site (in this case age over 18), then the user will also not release any private information as part of the proof of age transaction. One of the added benefits of government and private sector issued digital identity credentials and digital identity wallets is that the global community is working on paths to global interoperability of these services, allowing people to assert their credentials across borders. As the work of programs like (website: sidi-hub.community) proceed, we increase the ease with which visitors to the UK can be conformant with domestic UK laws on age verification increase, vice versa for UK residents travelling abroad, and crucially a shared paradigm for service providers operating within the UK and across borders to more easily deliver compliance with laws. This is analogous to the ease with which people globally can use credit & debit cards with NFC technology across borders to make payments and travel (e.g. NFC to board Transport for London buses and trains, NY Subway, Japan SUICA cards).
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 OpenID Foundation is of the view that systems generally should be end-user focussed and so in this context a single legitimate end-user should reasonably expect to be able to perform age assurance once by a mutually trusted entity and have that status communicated via a re-usable digital ID to a wide range of in scope service providers. This reduces the impact on

Question	Your response
	the individual in terms of UX friction, reduces the number of times the age assurance process needs to be done by the end-user and reduces the scope of the personally identifiable information that the individual would need to provide to multiple in-scope service providers. A critical requirement emerging from that end-user focus is that interoperability at a communication protocol level (not just format) is needed between digital ID providers and in-scope service providers. Without this there is a significant cost to the in scope service providers to integrate with a multitude of communication protocols. The simplest way to achieve the interoperability needed is to pick a very small number of standard communication protocols that meet the requirements of securely passing information in a privacy preserving manner and that the end-user is control of. It is worth noting that if user experience and interoperability were not a focus of government guidance, and a some or many proprietary solutions dominate than the risks to the ecosystem scale. For example, classic risks that emerge in absence of standards and processes that enable interoperability: (1) risk vendor and/or consultancy "lock-in" rises (2) the costs to serve usually rises for ecosystem participants, (3) the speed of adoption declines, and (4) the ability for ecosystem participants and government officials to ensure conformance drops. This is very similar to the requirements of Open Banking and re-usable digital identity systems. For reference Open Banking and re-usable digital identity systems around the world are using OpenID Connect with the FAPI profile as provided by the OpenID Foundation for this purpose. It has also worth noting that some OIDF standards are playing a material role in "government issued identity credentials" and in digital identity ecosystems run by public and private entities. For example, OpenID Foundation standards OpenID for Verifiable Credential Issuance, OpenID for Verifiable Credential Presentation, and OpenID Federation have been selected to be a core part of government solutions such as EU Digital Wallet Architecture Reference Framework (OID4VP, OID4VCI, SIOP v2), and other

Question	Your response
	issuing authorities such as the California DMV (OID4VP, OID4VCI), the Japanese Government (OID4VCI, OID4VC)., Italian Government (Federation) any many private entities as well.
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 The OpenID Foundation with its end-user centric vision would like there to be an illustrative case study where a re-usable digital ID is used. Not only does this approach deliver a better experience to legitimate end-users (e.g. present your age assurance in a couple clicks as easy as an Apple Wallet or Google Wallet transaction) but also is better from a data privacy perspective as the detailed interactions that are used to meet the age assurance duties only need to be performed with the end-users chosen digital identity provider rather than direct with potentially many in-scope service providers. This would enable in-scope service providers to more easily meet their obligations under the data protection act and their obligations under the Online Safety Act. It is worth noting that the economic models to underpin age verification services is still maturing. Traditional financial service KYC/IDA programs tend to involve complex waterfalls of processes to ensure compliance to regulation and ensure all (if not most) users can be served. In a similar way, users of age restricted content are likely to include all income profiles, diversity profiles, visitors to the country, users with accessibility concerns etc. As a result, relying parties are likely to structure “waterfalls” of services in the future to prioritize the lowest cost with the highest assurance and volume channel over the high cost, low assurance, and low volume channels. In that construct, relying parties may be interested in digital wallets and government-issued identity credentials that are low cost and progressively more available (e.g. in the US mDLs are issued at no cost to users or relying parties to accept, EU Digital Wallet large scale pilots in development now). The observations is that both the technologies, the commercial models, and information on how to circumvent the technologies are likely to evolve in the

Question	Your response
	short, medium and long term. Criteria and conformance may need to evolve as the marketplace and risks evolve.
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 The privacy obligations in the guidance are largely to comply with the current framework of laws, which are broad terms to apply to a wide range of use cases. However, in the narrow use case of age assurance for access to adult content, there are material risks of misuse. A relying party or service provider or wallet provider can use the existing framework of laws to develop an argument for the collection or retention of more data and it still leads to misuse (intentional or unintentional). Record keeping in Open Banking, Mobile Network, Digital Wallet and other Age Verification Services should be "blind" to the entity receiving the age assurance and the service provider brokering the transaction and the relying party should not be able to retain a history of the PII and where it was presented. For example: a financial institution using Open Banking takes receipt of information on the name of the user and the adult sites they visit in a way that is compliant with privacy law, age assurance law and user consent. The bank's internal algorithm determines (by crawling data of users), that individuals who access age restricted content frequently have lower credit worthiness. The bank updates its credit decisioning engine to the insight provided by the AI (without calibration for why the change is made) and lower credit lines or decline issuing credit to individuals that frequently request age assurance to restricted sites.
Question 9: Do you have any comments on our proposed approach to assessing compliance with the duties on service providers who publish or display pornographic	Confidential? – N The OpenID Foundation has no feedback regarding this question

Question	Your response
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 The OpenID Foundation has no feedback regarding this question
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 The OpenID Foundation has no feedback regarding this question

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