Consultation response form

Consultation title	Guidance for service providers publishing pornographic content
Representing (delete as appropriate)	Organisation
Organisation name	The Age Verification Providers Association

Your response

Note – in this response, we use "verification" to refer to the process of proving a user's age and "authentication" to refer to the process of confirming that the user is the same user who is being or has been previously verified.

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? – In part Confidential? – No We agree with the draft guidance on scope in general. **Tube sites** Further clarification would be helpful in relation to "Tube" sites, where approved partners of the publisher are able to upload content directly. They are not general users, but contracting parties who do so in return for revenue shares and referrals, and may even be considered as agents of the publisher. To the general public, such sites would often be the first they think of when they consider pornographic sites, and are not obviously user-to-user services. We believe they should be clearly within scope for Part 5. Regulating them under both Part 3 and Part 5 would create potential confusion from two separate regimes affecting a single site. Confidential? – Yes **[REDACTED]**
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? – No **Generative AI** We agree with 3.14 relating to generative AI. The adult industry expects to see the number of human performers fall considerably in 3 – 5 years' time, replaced by AI models. There is an overlap with the illegal harms guidance here, because GenAI can create content that appears to depict underage performers. Clearly such synthetic actors have no real age, so an alternative approach to exact age verification needs to be

Question	Your response
	adopted to ensure it is not depicting Child Sexual Abuse Materials. Fortunately, facial age estimation is already widely available and can provide results for real people within a mean average error of +/- 1 ½ years of their actual age, using state of the art solutions. Age estimation tools can be re-purposed as "age designation" tools for AI and used to monitor all novel content for underage performers. The test age for age designation would generally be set higher in this use-case than for highly effective age assurance because a 5% false positive rate at 18 is not acceptable for performers. This is achieved by raising the test age, increasing the buffer, and shifting the distribution curve of the results either side of the real age to the right, on a scale of age. The percentage of AI performers designated to appear under 18 should be set to tend towards zero. We recommend that Ofcom's guidance for age assurance of GenAI adult content require that age designation be designed to a very high level of assurance in terms of accuracy. The test age may reduce as these algorithms improve, without creating an unacceptable risk of false positives.
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? – No We welcome the use of a non-exhaustive list of examples as this facilitates innovation. We would encourage that the Ofcom list aligns with the Updated ICO's Opinion on Age Assurance for the Children's Code (January 2024) to ensure consistency in how both regulators are approaching age assurance. This includes the email address method as an example of a method that is highly effective as it fulfils the proposed criteria of accuracy, robustness, reliability and fairness (and has been certified by the Age Check Certification Scheme – see their registry https://www.accscheme.com/registry/kyc-avc-uk-ltd-verify-my-age)

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? – No **Accuracy** We strongly disagree with the statement that there is not "sufficient evidence as to the effectiveness and potential risks of different age assurance methods to recommend specific metrics for assessing whether or not any given age assurance method or process should be considered highly effective." The Age Check Certification Scheme conducted research for Ofcom and the ICO into the state of the art. It is also evidently possible to test any given method of age assurance to assess its effectiveness, both in terms of its headline false positive rate (wrongly determining a minor is 18 or older) and to a more sophisticated degree in terms of the distribution of errors either side of the true age. We are concerned that without expressing any opinion on the maximum acceptable false positive rate there will be a race to the bottom as sites which host primary priority content interpret the requirement as loosely as possible. Less accurate solutions are generally cheaper, and will also deliver a larger audience for sites whose commercial model is based on advertising and traffic volumes. **It is hard to see how Ofcom can defend in court action against a site that has deployed a solution which allows for up to 20% false positives, with perhaps 10% of them being more than 5 years below the age of 18, if the service provider has documented that that it considers this level of accuracy to be highly effective.** Ofcom may argue that 20% is too great a level of error, but would at that stage be forced to state what level is deemed sufficiently effective anyway.

Question	Your response
	Expected outcome approach to accuracy A simplified way to approach this is to set a minimum level of accuracy for the expected outcome of any given method or combination of method. For example: Highly effective age assurance systems must demonstrate that their certified expected outcomes are such that more than 95% of children under 18 are prevented from accessing primary priority content, and more than 99% of children under 16 are prevented. This has the benefit of being a neutral statement across all methods of age assurance. A clear signal to the market that, for example, 95% of young people under 18 should fail the test, and 99% of children under 16 should fail, would create a level playing field, but still leave services with a wide range of age assurance methods to choose from. Those who use less accurate age estimation solutions would simply need to increase the test age to widen the buffer between it and 18, so as to gain certification that they meet these minimum criteria. **Robustness** The observed outcome may diverge from the expected outcome as a result of fraud (borrowed credentials, borrowed facial images). In some use-cases for digital identity, regulations are set to combat fraud. This adds cost and complexity, and if applied for Part 5 could also be a deadweight to widespread voluntary adoption, as it may create too much friction in the user-acquisition process for Part 5 sites to tolerate. We do not recommend that Ofcom calibrates its requirements for highly effective age verification to seek to eliminate fraud at this stage. This is where the concept of ensuring that provider pornographic content "not normally" encountered is applicable (per Section 81 (2) of the Act)[1]. Only when

[1] **Duties about regulated provider pornographic content**

Question	Your response
	a fraud is widespread and therefore undermines that goal substantially, should a method be deemed to fail to meet the minimum requirement for accuracy we set out above (the 95% for 18 and 99% for 16 rule), and additional countermeasures be required. . **Reliability** We agree with the guidance around assessment of variance, and performance monitoring. Any method that relies on remote verification of identity documents and/or liveness or self-images should have baseline measures in place to combat both presentation attacks and AI-generated deepfakes where such opportunities are widely and cheaply available to minors. Solutions that make no attempt to combat such attacks are unlikely to be considered reliable, and could therefore fail the "not normally accessible" requirement. **Fairness** We agree that age estimation methods reliant on machine learning should use diverse training datasets that reflect the population likely to be tested. An Age Assurance System or component is fair if protected groups receive an equal proportion of positive outcomes, or an equal proportion of errors. **We recommend in the longer term that Ofcom sets a tolerance level for outcome error parity for highly effective age assurance**, thus acknowledging that no such method can eliminate bias entirely, but ensuring it is not at a significant level which has an observable impact on any group of users with protected characteristics. **Initially, we believe it would be sufficient to require that digital service providers are aware of this metric and publish the expected outcome for their system(s).**

"A duty to ensure, by the use of age verification or age estimation (or both), that children are not normally able to encounter content that is regulated provider pornographic content in relation to the service."

Question	Your response
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? – No We address below the concern that some methods can be easily circumvented by a child using an adult's personal details, setting out mitigations: **Open banking** – it is unlikely – and would be financially rash – for an adult to share access details to their online banking so this is robust for Part 5. If the user then creates a separate account, so the online banking is not re-used each time the log on, then regular re-authentication via the bank should be required to prevent extended misuse by a user initially given access by an adult. **Photo-ID matching** – with suitable measures to prevent deepfake injection and presentation attacks, this is also robust, but periodic re-authentication is required to prevent a user borrowing an adult for enrolment from avoiding detection. **Facial age estimation** – it is equally possible to "borrow" an older face at the point of access or enrolment, so regular re-authentication should be required if a Facial Age Estimation (or other biometric) is to provide access for future sessions. In both these above two methods, the period allowed between authentications determines the degree of robustness. A period between 1-3 months would not be an excessive interruption to the user experience. **Mobile Network Operators** – adult CRF SIM blocks The network's process for removing adult CRF SIM blocks would need to be audited to provide assurance that this is only possible as a result of a reliable age or identity verification process. Regular re-verification should be considered to mitigate the risk from phones being handed-down to minors. **Mobile Network Operators** – Customer records As for banks, MNOs hold customer identity data, potentially including age acquired during the sales process. So, even without the CRF being lifted, a user may be able to verify their age using their MNO data. These MNO customer take-on processes would need to be audited to provide assurance that the customer data used for account creation is based on reliable

Question	Your response
	identity proofing. Regular re-verification should be considered to mitigate the risk from phones being handed-down to minors. **Credit card** – Two factor bank-level authentication is now generally required for payment authorisations which prevents a child simply borrowing a credit card. Alternatively, a micropayment (1p) to the card will ensure the age verification provider appears on the adult's statement, highlighting any impersonation. **Email address** – the owner of the email address must be in control of its inbox and authenticate by responding to a message from the AV provider, and periodic re-authentication may also be applied. The design of such solutions should be such that it is unlikely the owner of the address would be willing to give permanent access to a minor to that inbox e.g. the address has been used for high value/risk purposes such as a mortgage application. **Digital Identity Wallets** – these must use biometric authentication that is uniquely tied to the user which created the identity. Note: Some smartphones allow for a second face or fingerprint to be added giving not reliable indication the wallet is being used by its rightful owner. Other methods of age assurance appropriate to other use-cases can be suitable only if they are augmented with additional authentication measures: **Credit reference agency** – a knowledge-based authentication where the user knows some details of their credit record (the date on which their rent or mortgage is paid), or a cross-check with a second means of verification e.g. a drivers' licence number should meet the robust requirement Ofcom seeks. **Electoral roll** – a cross-check with a second means of verification e.g. a drivers' licence number could meet the robust requirement Ofcom seeks. (In general, multiple checks of different source data will give increased levels of assurance). Rather than Ofcom seeking to define countermeasures for any given method, it should

Question	Your response
	require that methods meet the minimum requirement for highly effective age assurance, and monitor to ensure that service providers put surveillance in place to ensure their services cannot normally be encountered by children through methods of circumvention becoming widespread.
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? – No **Accessibility** We note that interoperability is an important mechanism to promote accessibility, as a user need only fine one method which is accessible to them, and can use it across multiple services. Re-usability has a similar, if less extensive benefit, particularly where a user needs assistance when an age check is first completed e.g. helping a blind person position their face correctly for an estimation process. **Interoperability** The guidance should more clearly endorse interoperability to reassure services that, if they make use of a well-designed interoperability network, their level of compliance using an indirect mechanism can be judged to equal age assurance conducted through a single direct supplier. We are concerned services may be reluctant to place reliance on checks carried out by third parties with whom they do not have a direct contractual relationship, which is the underlying basis of interoperability, unless the regulator gives a clear signal that, provided the network applies due diligence to its participating AV providers, and all the methods relied upon for Part 5 meet the defined minimum level of accuracy for highly effective age assurance, that the benefits of interoperability should be considered to outweigh any additional risks.

Question	Your response
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? – No We note that the case study reflects current operational good practice accurately.
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? – No Service providers who use a third-party age assurance provider should be permitted to cross-reference records held – and updated – by the third party. The third party may make frequent improvements and changes to the detailed operation of the age assurance system and it would be duplicative and potentially lead to version control errors if service providers replicate this source records data.
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 content, including on the proposed examples of non-compliance? Please provide any information or evidence in support of your views.	Confidential? – No **We note that there are some 4-5 million pornographic websites available online.** The vast majority are based overseas. Many will no have a contact point, and their ownership may be opaque. The Online Safety Enforcement Guidance may not be comfortably applied to the adult industry beyond a small number of high-profile sites. **The importance of creating a level playing field from day one, where all sites are at risk of business disruption measures cannot be over-emphasised.** Targeting only the largest sites will provoke extensive legal objections because these sites will fear – with some justification based on the experience in other jurisdictions such as France and Germany – that their traffic will almost entirely (>99% is reported by Aylo for certain US states) not attempt age verification and may defect to other sites not targeted by the regulator. They therefore face an existential threat and have no choice but to invest heavily in legal defence to delay the impact of the Act.

Question	Your response
	Ofcom must therefore diverge from a basic pareto approach to the targeting of enforcement action at a few large sites, and drive compliance at all levels of the adult industry at the outset of the regime. This is not aligned to the modus operandi of regulators in other fields, or indeed to other sectors, but reflects the unique nature of the online adult sector, and the very high substitution rates exhibited by consumers in the face of any friction to their user experience. We also know that the adult industry is not opposed to the introduction of highly effective age assurance PROVIDED it is enforced universally. So, both messaging and action must reflect and determination by the regulator to apply the Act to all sites accessed from the UK to any significant degree, from the first day that its powers become effective. We note that the European Commission moved swiftly as soon as its powers to directly regulate Very Large Online Platforms came into force to make information requests that are the first step in the enforcement process. This sent a loud and clear message to platforms that the Commission expected them to comply with legislation as and when it came into force. This has secured focus, and empowered trust and safety professionals within all services to make the case for action. Sadly, compliance for many businesses is not a question of doing the right thing, but rather of weighing the costs of compliance with the risk of being fined, and assessing the balance of the business case. **If the perceived risk of enforcement remains zero for any period after legislation comes into force, then the business case will not meet the threshold for action and the positive impact of the Act will be delayed.**
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? – No We can confirm that the age assurance industry has experienced a downward trend in its pricing over the past five years, as a result of technical innovation and increased competition. We expect this trend to

Question	Your response
	continue and to be further affected by the introduction of interoperability.
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? – No We would expect our members to provide their services, and the notices that explain them, in Welsh as well as English where they are accessed from users located in Wales.

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