Highly Effective Age Assurance – Frequently Asked Questions (FAQ)*

For details of services which fall out of the scope of Part 5, please visit page 8 of our Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services

Q: What is the purpose of Ofcom's Guidance on age assurance?

A: The guidance aims to ensure that online services which publish pornographic content implement effective measures to prevent children from accessing such material, in line with the Online Safety Act 2023.

Q: Who does the guidance apply to – which services fall under Part 5 of the Act?

A: A service falls within Part 5 of the Online Safety Act if it meets **all** of the following criteria:

i. The service publishes or displays regulated provider pornographic content, as defined in section 79(2) of the Act.

ii. The service is within the scope of Part 5 and is not exempt.

iii. The service has links to the UK, meaning it either has a significant number of UK users or the UK is one of its target.

Q: What is considered to constitute a 'significant' number of UK users?

A: The Online Safety Act does not define what is meant by a 'significant number' of UK users. Service providers should be able to explain their judgement, especially if they think they do not have a significant number of UK users.

Q: What are the key duties for service providers under Part 5 of the Online Safety Act?

A: The key duties for services under Part 5 are to:

- implement age assurance measures that are 'highly effective' at correctly determining whether a user is a child (under the age of 18) or not;
- ensure that children are not normally able to encounter pornographic content on their regulated service (i.e., by using an effective access control measure);
- make and keep written records of the age verification or estimation methods used; and
- publish a publicly available statement summarising the written records including details of the age verification or estimation methods employed.

Q: What criteria ensures an age assurance process is 'Highly Effective?

A: To be considered highly affective, age assurance methods must be of a kind that could be highly effective at correctly determining whether or not a user is a child. Service providers should ensure that the process fulfils each of the following four criteria:

Technically accurate	The degree to which an age assurance method can correctly determine the age of a user under test lab conditions.
Robust	The degree to which an age assurance method can correctly determine the age of a user in actual deployment contexts.
Reliable	The degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.
Fair	The extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.

Q: Which methods of age assurance are capable of being highly effective?

A: Highly effective age assurance refers to methods that accurately determine a user's age, to ensure that children are not normally able to access pornographic content. Acceptable methods **may** include, but are not limited to:

- Photo-ID matching – comparing a user's uploaded ID to an image of the user, to verify that they are the same person.
- Credit card checks.
- Open banking – with the user's consent, age information held by a bank is shared with the service.
- Facial age estimation through using technologies which perform facial analysis.
- Mobile-network operator (MNO) age checks.
- Digital identity wallets, which enable users to verify and securely store their attributes, such as age, in a digital format. This verification may take place using a variety of methods, including those listed above.

Q: Are there any age assurance methods that are not acceptable?

A: Yes, methods that are **not** considered as highly effective include:

- Self-declaration of age
- Request for a date of birth be entered without additional verification
- Age verification through online payment methods which do not require a user to be over the age of 18 (e.g. debit cards)
- General contractual restrictions on the use of the service by children (e.g. terms and conditions, text warnings on content, or general disclaimers on entry to the website).

Q: Why is a self-declaration of age not considered 'highly effective age assurance'?

A: Self-declaration is **not** considered to be highly effective age assurance as it is not considered to meet Ofcom's four criteria (technically accurate, robust, reliable, fair) .

Q: Are there any approved third party providers? Do you recommend any specific third-party application for age verification?

A: Ofcom do not approve third party providers of highly effective age assurance and are unable to recommend specific providers of age verification technologies. When choosing a provider, services should ensure the relevant checks are carried out to assess if the method is highly effective, taking account of Ofcom's Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services.

Q: What about privacy and data protection rules - do these still apply?

A: Yes, privacy and data protection rules still apply when implementing age assurance measures. We've worked closely with the Information Commissioner's Office (ICO) to adopt an integrated approach, ensuring compliance is supported with our respective regulatory regimes. Our guidance sets out where services should consult ICO guidance for further information on data protection requirements.

Compliance by service providers with both the online safety and the data protection regime is mandatory and should not be considered a trade-off.

Q: Do users need to pass age verification for each occasion they access the site?

A: When considering whether users need to pass age verification for each new / repeat visit to a site which displays or publishes pornographic content, services should consider Ofcom's criteria for highly effective age assurance (technically accurate, robust, reliable and fair). We expect service providers to identify and take appropriate steps to mitigate against methods of circumvention that are easily accessible to children, and where it is reasonable to assume that children may use them.

Q: Does explicit text content (e.g. descriptions of pornographic / adult content) need to be excluded from pages which can be accessed without highly affective age assurance in place?

A: No, content is not caught by the Online Safety Act if it:

i. Consists only of text
ii. Consists only of text accompanied by:
    a. a GIF which itself is not pornographic content; and/or
    b. an emoji or other symbol

Details can be found at section 79 of the Online Safety Act.

Q: Is there a system that allows users who have already verified their age on one site to access another site without needing to verify their age again?

A: Services may consider the use of digital identity services. Such services provide a digital representation of a person which enables them to prove who they are during interactions and transactions online and in person. Reusable digital identities are those which can be used multiple times for different interactions and transactions. This includes digital identity wallets which enable users to verify and securely store their attributes (such as age) in a digital format. Once their identity or an attribute of their identity has been verified and stored in the wallet, a user may choose to share individual attributes, such as their age, or their status as an adult, with a relying party.

Q: If a UK user accesses the service through a VPN or TOR (software that allows the user to access sites anonymously and masking which country they are accessing it from), would the service be considered to be in breach of their duties?

A: We expect service providers to take steps to mitigate against, and refrain from promoting, any circumvention techniques which are easily accessible to children and where it is reasonable to assume they may use them. In addition, service providers should not host or permit content on their service that directs or encourages child users to circumvent the age assurance process or the access controls, for example by providing information about or links to a virtual private network (VPN) which may be used by children to circumvent the relevant processes.

Q: What happens if the UK are geo-blocked from my service?

A: The Online Safety Act applies to services with links to the UK. This applies where the service has a significant number of UK users, or the UK forms one of, or the only, target market for the service.

However, there are a few things to consider:

- Effectiveness of geo-blocking – if UK users can still access the site (e.g. through weak geo-blocking), then Ofcom may find that the service falls within scope of the Act.
- Intentional targeting – if a service geo-blocks the UK but markets to UK users (e.g. UK-specific content) again, the service may still be within scope of the Act.

Q: What are the consequences of non-compliance?

A: The Online Safety Act gives Ofcom the power to take enforcement action for non-compliance with their Part 5 duties, including imposing financial penalties of up to £18 million, or 10% of qualifying worldwide revenues (whichever is greater).

Our Online Safety Enforcement Guidance sets out procedures we will follow where we suspect non-compliance with the obligations that apply to service providers under the Act.

Q: Is forwarding all UK traffic to an alternative, non-adult site considered an acceptable solution?

A: Under the Online Safety Act, 'Provider pornographic content' refers to pornographic content published or displayed on an internet service either by the provider or by someone acting on their behalf.

When implementing such measures, a service should consider the effectiveness – if UK users can still access the initial site, then Ofcom may find that the service falls within scope of the Act.