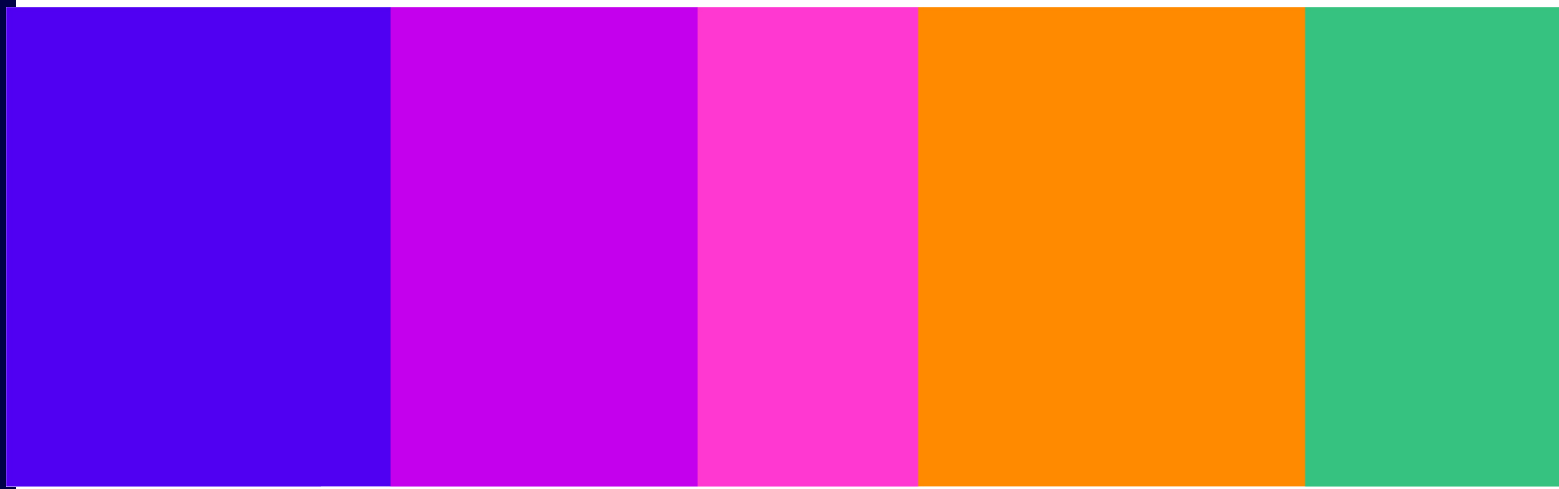


Rapid assessment of highly effective age assurance at 16

[Welsh version available](#)

Published 29 October 2026



Contents

Section

1. Introduction.....	5
2. The role of highly effective age assurance in implementing the new age restrictions	8
3. Assessment of available age assurance methods	13
4. How could age assurance processes be strengthened?	27
5. Next steps.....	32

Overview

This rapid assessment considers what highly effective age assurance could look like for determining whether someone is 16 or over. We have produced it ahead of the Parliamentary debate on the UK Government's forthcoming regulations on age restrictions for online services, which include restrictions on under-16s accessing social media services and certain risky features and functionalities.

The UK Government's proposals are part of a broader international move towards age restrictions on children's social media access. The government has stated that highly effective age assurance, instead of the "reasonable steps" criteria applied in Australia, will be critical for the successful implementation of the ban. This is designed to make it harder for children to bypass safeguards.

We have based this assessment on the criteria and principles set out in our existing guidance on highly effective age assurance at 18. We have therefore assessed methods against the criteria of technical accuracy, robustness, reliability and fairness, and considered the principles of accessibility and interoperability. Our existing guidance sets out seven age assurance methods capable of being highly effective at 18.

Our assessment has identified four age assurance methods capable of being highly effective at determining whether someone is 16 or over: photo ID matching, digital identity services, banking-based checks and facial age estimation. This means there is currently less choice of highly effective methods at 16 than 18, and our rapid assessment has not surfaced emerging methods that would be ready before the ban comes into force. The market may develop new and innovative solutions once new age restrictions are in place, and we will continue to monitor emerging developments in the market.

16- and 17-year-olds are more likely than over-18s to need access to a photo ID and those without would likely need to take steps to obtain one to access age-restricted services. This is because, of the methods identified in this rapid assessment for highly effective age assurance at 16, photo ID is either required as part of the method itself, or as the likely backstop for other methods, such as facial age estimation.

The new age restrictions will also impact adult users of social media services, including the largest services widely used by people in the UK. To prevent under-16s from accessing these services or accessing certain features, many adults are also likely to have to demonstrate that they are above that age. Social media services can use the wider range of methods we identified in our existing guidance to determine whether users are over 18, and some users with existing accounts may not need to complete an age check if the service already holds accurate and reliable information to establish they are over the required age.

Introducing age assurance at 16 will involve the processing of additional personal data. However, available methods can be delivered in a way that protects users' privacy and complies with data protection law. We will continue to work closely with the Information Commission in considering these implications.

No age assurance method is completely robust against circumvention by children. Social media services will need to implement highly effective age assurance in full, including taking practical measures to tackle circumvention by children. Correctly implementing highly effective age assurance should significantly reduce the likelihood of under-16s accessing restricted services or functionalities. However, we expect some children will

attempt to get around age checks, including through the use of VPNs. We have identified some ways services could mitigate circumvention risks, such as reporting of underage users. We will monitor circumvention by children and will publish a report on circumvention within twelve months of the ban coming into effect.

Current age inference methods cannot act as an age gate. Because these models rely on user activity on a platform for a period of time to estimate age, they are not suitable as the main way to prevent new under-16 users from accessing services in scope of the ban. However, age inference models may still have a supporting role to play as part of a wider age assurance system – for example, to help detect under-16s that have bypassed a highly effective age check.

It is the responsibility of regulated services to ensure their new age assurance processes are highly effective. While we expect to see further innovation from the whole tech industry to support the implementation of highly effective age assurance at 16, questions around governance, accountability and effectiveness of such interventions are out of scope of this report. Today, we have also published our [statutory report on app stores](#), which is designed to inform the government’s decision on whether to bring app stores into scope of the Online Safety Act. Regardless of any future regulatory role for app stores, or other actors in the ecosystem, regulated services will need to demonstrate that their overall age assurance process is highly effective to comply with any new obligations.

Ofcom is now developing draft guidance for services as part of our preparations for implementation of the proposed social media ban for under-16s. As soon as the expected restrictions are introduced to Parliament, we will consult on guidance on highly effective age assurance at 16 to help services understand and comply with their future obligations. Additional methods that are capable of being highly effective at 16 may be identified as part of the consultation.

1. Introduction

- 1.1 In June 2026, the UK Government announced a package of age restriction measures intended to strengthen protections for children online. These include banning social media providers from offering services to under-16s.¹ They also include restricting under-16s' access to features like livestreaming and strangers communicating with children, while ensuring these features are turned off by default for 16- and 17-year-olds.² In July 2026, the Government announced further measures for 16- and 17-year-olds.³ It has made clear that highly effective age assurance will be crucial to implementing these measures.⁴
- 1.2 Under [the Online Safety Act 2023 \(the Act\)](#), certain user-to-user services (Part 3 services) are already required to use highly effective age assurance to determine whether or not a user is a child, i.e. whether a user is over 18.⁵ Our [April 2025 Statement on Protecting Children from Harms Online](#) (April 2025 Statement) and our [Guidance on Highly Effective Age Assurance for Part 3 services](#) (existing HEAA Guidance) set out our approach to highly effective age assurance.⁶ In July 2026 we published our statutory [Report on the use of age assurance](#) (age assurance report), which assessed how regulated services are using age assurance and how effective it has been for the purpose of complying with their duties.⁷
- 1.3 To help inform Parliament's consideration of the forthcoming draft regulations, the Secretary of State requested that Ofcom undertake a rapid assessment of what highly effective age assurance looks like for determining whether someone is 16 or over.⁸
- 1.4 This preliminary assessment sets out a non-exhaustive list of the age assurance methods that we consider are capable of being highly effective for determining whether someone is 16 or over, including new and emerging methods.⁹ We have assessed these methods against the criteria of technical accuracy, robustness, reliability and fairness. We have also considered the principles that age assurance should work effectively for all users (accessibility) and interoperability, as well as potential privacy and data protection implications. This assessment also discusses circumvention and displacement risks, and the role that other actors in the digital ecosystem could play in strengthening age assurance.

¹ Department of Science, Innovation and Technology (DSIT), 2026. [Social media to be banned for under-16s in landmark government move to give kids their childhood back](#). [accessed 26 August 2026].

² DSIT, 2026. [Social media to be banned for under-16s in landmark government move to give kids their childhood back](#). [accessed 26 August 2026].

³ DSIT, 2026. [New social media curfews and crackdown on addictive features to better protect 16- and 17-year-olds online](#). [accessed 26 August 2026].

⁴ DSIT, 2026. [Growing up in the online world: progress statement \(June 2026\)](#). [accessed 26 August 2026].

⁵ Under the [Online Safety Act 2023](#) (the Act), Ofcom is the UK regulator for online safety. A child is defined at section 236(1) of the Act as "a person under the age of 18".

⁶ Ofcom, 2025. [April 2025 Statement: Protecting Children from harms online](#) (April 2025 Statement). Ofcom, 2025. [Guidance on highly effective age assurance for Part 3 services](#). Part 3 services are regulated user-to-user and search services. The Part 3 guidance follows the same approach as our guidance for Part 5 services, which are providers that publish or display their own pornographic content.

⁷ Ofcom, 2026. [Report on the use of age assurance](#).

⁸ DSIT, 2026. [June progress statement: letter from DSIT Secretary of State to Ofcom Chair and CEO](#). [accessed 26 August 2026].

⁹ As defined in section 230 of the Act, age assurance includes both age verification and age estimation. Age verification means any measure designed to verify the exact age of users of a regulated service. Age estimation means any measure designed to estimate the age or age-range of users of a regulated service.

- 1.5 Alongside the UK Government’s proposals, there is a broader international move towards introducing age-based restrictions on children’s access to social media.¹⁰ In Australia – the first country to implement an age-based restriction of this kind – the social media minimum age (SMMA) obligation requires providers of age-restricted social media platforms to take “reasonable steps” to prevent Australian children under the age of 16 from having accounts.¹¹ The UK Government announced that it plans to use “the same model for a social media ban as Australia”, but intends to “learn the lessons from Australia’s experience by introducing more highly effective age assurance (HEAA) measures to support compliance”.¹² This is designed to make it harder for children to bypass safeguards.
- 1.6 This rapid assessment has been conducted between June and October 2026, drawing on publicly available evidence, our engagement with relevant stakeholders including those from the age assurance industry, service providers and international regulators, and our experience of regulating in relation to the duties to use highly effective age assurance under the Act. It is intended to help inform parliamentary debate on the draft regulations, rather than to act as guidance to assist services in implementing highly effective age assurance to comply with these regulations. We expect to consult on draft guidance on highly effective age assurance at 16 in the coming months, following the introduction of the draft regulations into Parliament.
- 1.7 This document does not assess the impacts of using highly effective age assurance at 16 to implement a social media ban and potential other restrictions. It is for Parliament to consider the impacts of the potential new duties themselves. Ofcom will publish an impact assessment when we consult on our draft guidance on highly effective age assurance at 16, focusing on the areas over which we may exercise discretion.
- 1.8 The assessment is structured as follows:
- **Section 2** explains our existing approach to highly effective age assurance and how it can be used to apply restrictions to under-16s.
 - **Section 3** sets out the age assurance methods we consider are capable of being highly effective at determining whether someone is 16 or over and discusses if these methods can work effectively for all users. It also discusses new and emerging methods.
 - **Section 4** discusses how age assurance could be strengthened, including circumvention and displacement risks and the role of wider actors in supporting implementation.

¹⁰ A number of jurisdictions have passed, are in the process of passing, or have announced their intention to pass legislation to prevent children from accessing certain social media services. For example, the European Commission has proposed the EU KIDS Act, which establishes a harmonised minimum age of 15 for independent social media accounts, while a number of European countries, including France, Greece and Austria, are also pursuing age-based restrictions for minors’ access to online services. For a current list of global social media age restrictions updates see Jahangir, R. and Hendrix, J., 2026 [Tracking Efforts to Restrict or Ban Teens from Social Media Across the Globe](#), Tech Policy Press, 23 February. [accessed 8 September 2026].

¹¹ Section 63D of Australia’s Online Safety Act does not prescribe what ‘reasonable steps’ platforms must take or set a specific age assurance requirement, however eSafety guidance makes clear that services are expected to implement “some form of age assurance, see Australian Government Federal Register of Legislation, 2024. [Online Safety Amendment \(Social Media Minimum Age\) Act 2024 - Federal Register of Legislation](#). [accessed 26 August 2026].

¹² DSIT, 2026. [Social media to be banned for under-16s in landmark government move to give kids their childhood back](#). [accessed 26 August 2026].

- **Section 5** sets out the next steps, including how Ofcom is preparing to implement the expected new age restrictions.
- **Annex 1** contains a glossary of key terms.

2. The role of highly effective age assurance in implementing the new age restrictions

Our approach to highly effective age assurance

- 2.1 The Secretary of State has requested that Ofcom assess what highly effective age assurance looks like for determining whether someone is over 16. In this section we explain our current approach to highly effective age assurance, as well as the role it could play in securing compliance with the expected new age restrictions.
- 2.2 Our existing HEAA guidance sets out criteria and principles to assist providers in implementing a highly effective age assurance process.¹³ As we set out in our [January 2025 Age Assurance and Children's Access Statement](#) (January 2025 Statement), each criterion is important and a service's age assurance process needs to fulfil all four criteria to be considered highly effective.¹⁴ Alongside fulfilling the criteria, services should consider the principles of accessibility and interoperability when implementing an age assurance process, as well as ensure that their process is compliant with data protection law.

Highly effective age assurance criteria and principles

- 2.3 We have produced this assessment following the criteria and principles-based approach set out in our existing HEAA guidance as we expect the same approach to be relevant at 16. Tables 1 and 2 set out these criteria and principles and what they mean in practice. We will develop and consult on draft guidance on highly effective age assurance at 16, once the government's expected draft regulations are published in the coming months.

Table 1: Criteria that a highly effective age assurance process must fulfil

Criterion	Description	What does this mean in practice?
Technical accuracy	The degree to which an age assurance method can correctly determine the age of a user under test lab conditions.	This means ensuring that methods have been evaluated against appropriate metrics and are periodically reviewed for improvements. In the case of age estimation methods, a challenge age approach should be used.
Robustness	The degree to which an age assurance method can correctly determine the age of a user in actual deployment contexts.	This includes taking steps to consider and mitigate circumvention techniques specific to each method. For example, any method that involves capturing a photo of a user should include liveness detection technology. ¹⁵

¹³ Ofcom, 2025. [Guidance on highly effective age assurance for Part 3 services](#).

¹⁴ Ofcom, 2025. [January 2025 Age Assurance and Children's Access Statement](#) (January 2025 Statement), pp.31-54.

¹⁵ Liveness technology is a feature used to ensure that the face being analysed is not a photograph, video, or any other form of spoofed representation.

Criterion	Description	What does this mean in practice?
Reliability	The degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.	This includes taking appropriate steps when age assurance methods rely on artificial intelligence or machine learning to ensure it is regularly tested, monitored and assessed, as well as steps to ensure that any data relied upon as part of the age assurance process comes from a trustworthy source.
Fairness	The extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.	This includes, for example, ensuring methods which rely on artificial intelligence or machine learning are trained and tested on diverse population data and evaluated so that the method(s) does not produce significant bias or discriminatory outcomes.

Table 2: Principles that should be considered when designing a highly effective age assurance process

Principle	Description	What does this mean in practice?
Accessibility	The ability of a method or process to work for all users.	This includes considering the potential impact that the chosen age assurance method(s) might have on users with different characteristics; the variety of age assurance methods a user may be able to choose from; and the user journey through the age assurance process to be accessible to people with a wide range of physical and intellectual abilities.
Interoperability	The ability of technological systems to communicate with each other using common and standardised formats.	This may involve re-using the result of an age check across multiple services to allow different providers of age assurance methods to share the information, provided this is done in line with data protection laws. Interoperability offers a potential benefit to the user experience, as it limits the amount of information that users need to provide when accessing a new service if they have already proved their age elsewhere. This could reduce the time and effort required by users to understand, and input into, different age assurance processes.

Privacy and data protection

- 2.4 Our existing HEAA guidance also sets out how providers can have regard to protecting users' privacy when implementing age assurance.¹⁶ All age assurance methods involve processing personal data and are therefore subject to UK data protection requirements. As noted in our existing guidance and [Joint Statement with the Information Commission \(ICO\)](#), services must ensure that any age assurance methods they use are necessary, effective and proportionate, comply with UK General Data Protection Regulation (GDPR) principles, and do not create risks to users' rights and freedoms that outweigh their benefits.¹⁷ These same

¹⁶ Ofcom, 2025. Guidance on highly effective age assurance, pp.22-24.

¹⁷ More information about services' data protection obligations when implementing age assurance can be found in our 2026 [Joint Statement with the Information Commission \(ICO\)](#), p.8. Also see ICO. [Age Assurance Opinion Piece](#). [accessed 26 August 2026].

principles will apply to any age assurance processes introduced for the purposes of new age restrictions.

Data protection considerations for implementing age restrictions at 16

- 2.5 The use of highly effective age assurance for implementing the upcoming age restrictions will involve the processing of personal data and therefore raises a range of data protection considerations. The considerations set out in the Joint Statement with the ICO continue to reflect the ICO's current position on the use of age assurance to prevent access to a service by children under the minimum age.
- 2.6 Regardless of which age assurance mechanism service providers choose and whether they are processing a child's or adult's personal information, services must follow the data protection principles.¹⁸ Any personal data processed by services when implementing age assurance must be limited to what is necessary and proportionate to achieve the purpose of the processing. Providers must ensure that age assurance methods balance the level of certainty required about a user's age with the principles of necessity and data minimisation. Given that the potential new regulations would apply to specific age groups of children, the service would need to have sufficient certainty of a user's age to process their data lawfully and apply the appropriate protections.¹⁹
- 2.7 The ICO's [Age Assurance Opinion](#) explains how services can use age assurance technology in compliance with data protection law in a risk-based and proportionate way.
- 2.8 Further consideration would be needed regarding how service providers should handle existing accounts belonging to users under 16 in a way that meets their data protection obligations.²⁰ This includes:
- a) Whether there is a valid lawful basis to process underage users' personal data to maintain their account;²¹
 - b) Where services retain existing account data, how that data should be handled, including preventing it being used for secondary purposes, deleting it in the event a user does not reactivate their account, and being transparent with users about how it is handled; and
 - c) How underage users can exercise their data subject rights in relation to any data that is retained.
- 2.9 A key transparency requirement under UK GDPR is that individuals have the right to be informed about the collection and use of their personal data. Recent research from the ICO found that fewer than half of children (45%) say they understand what happens to their personal information when they share it on a game, app or website.²² Service providers must provide users with privacy information including the purpose for processing their

¹⁸ The UK GDPR sets out seven key principles: lawfulness, fairness and transparency; purpose limitations; data minimisation; accuracy; storage limitation; integrity and confidentiality, and accountability. ICO. [A Guide to the data protection principles](#). [accessed on 30 September 2026].

¹⁹ ICO. [Age Assurance for the Children's Code](#), 6.1.5 Data Minimisation. [accessed 26 August 2026].

²⁰ In Australia, services were instructed to remove accounts belonging to users under the age of 16 but some platforms could choose to deactivate accounts so that they could be reactivated when the user turns 16. See eSafety Commissioner. [How do the social media age restrictions affect me?](#). [accessed 26 August 2026].

²¹ The ICO states that providers must not keep personal data for longer than they need it, periodically review the data held, and consider any challenges to the retention of data. See [Principle \(e\): Storage Limitation](#). [accessed 26 August 2026].

²² ICO, 2026. [Children's and Parents' Attitudes on Information Rights](#), p.20.

personal data, data retention periods and who personal data will be shared with. They must also provide the information in a way that is concise, transparent, intelligible, easily accessible and uses clear and plain language.²³

The role of highly effective age assurance in implementing new age restrictions

What are the expected use cases for highly effective age assurance?

- 2.10 To comply with the new age restrictions, we expect that in-scope service providers will need to use highly effective age assurance to determine:
- whether a user is 16 or above to ensure that the relevant restrictions are applied to under-16s; and/or
 - whether a user is 16 to 17 to ensure that certain default settings are applied to those users.
- 2.11 In-scope service providers may also need to use highly effective age assurance to determine whether a user is 18 or above in order to comply with the existing children’s safety duties.
- 2.12 The methods and processes that would be appropriate for determining a user’s age or age range will depend on the age restrictions a service provider needs to comply with. Where there are both adults and children on a service, we expect a service could offer a range of age assurance methods that are capable of being highly effective at 18 as well as at 16, to provide more choice for users depending on the use case.

Will all existing users need to complete a highly effective age assurance check?

- 2.13 Not all existing users will need to immediately complete a highly effective age check to determine whether they are 16 or over. Providers may already hold information on existing users that could be used to help determine someone’s age or age range.²⁴ Using reliable age information that services already hold about a user could help reduce friction and preserve user privacy, by reducing the number of new age checks that need to be completed.
- 2.14 To determine which users may not need to immediately complete a new highly effective age assurance check, services could use a range of information relating to an existing user’s account.²⁵ Examples include:
- **Results of a highly effective age check** that has previously been conducted, for example to determine whether a particular user is over 18. As set out in our existing HEAA guidance, service providers should consider whether repeated age checks are needed to secure the robustness of their age assurance process.²⁶

²³ ICO. [Right to be informed](#). [accessed 29 September 2026].

²⁴ DCMS, 2026. [Fact sheet: New rules to protect children online - GOV.UK](#). [accessed 8 September 2026].

²⁵ There are specific data protection considerations for services when reusing personal data and services must ensure that any personal data is reused in line with their data protection obligations regarding compatibility and the reuse of personal information. See the ICO’s updated guidance on purpose limitation: [Principle \(b\): Purpose limitation | ICO](#). [accessed 29 September 2026].

²⁶ Ofcom, 2025. Guidance on highly effective age assurance, p.16.

- **How long a user's account has existed (account tenure)**, provided that this information is used as part of a highly effective age assurance process. In particular, the service would need to be satisfied that the account has belonged to the same user throughout its tenure and that it holds no information indicating a change of ownership.

2.15 We intend to provide more information for services on how existing information can be used, including considerations of how long an account needs to have existed for in relation to account tenure and other measures to ensure robustness, as part of our consultation on our draft guidance.

3. Assessment of available age assurance methods

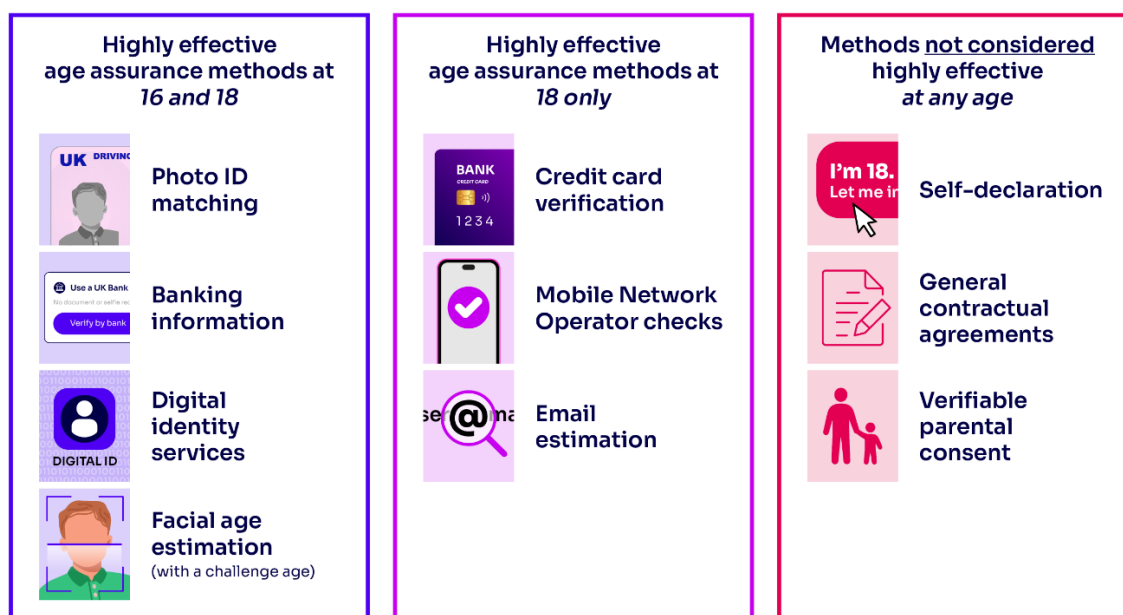
What age assurance methods have we assessed?

- 3.1 Our existing HEAA guidance sets out a non-exhaustive list of age assurance methods that we consider are capable of being highly effective at correctly determining whether someone is 18 or over.²⁷
- 3.2 We used the methods in our existing guidance as the starting point for our assessment of highly effective age assurance at 16. We have assessed each method against the criteria of technical accuracy, robustness, reliability and fairness, and have considered the principles of accessibility and interoperability, and how each method may impact user privacy.
- 3.3 Based on the evidence currently available, our preliminary assessment suggests that there are four methods capable of being highly effective at correctly determining whether someone is 16 or over. Our assessment also discusses three additional methods that are capable of being highly effective at 18, but not at 16. These methods could be offered to adults as part of a service's age assurance process, as if a user is 18 or over, it follows that they would also be over 16. We also set out the methods that are not capable of being highly effective at any age.
- 3.4 We have also considered new and emerging methods to support highly effective age assurance at 16 in the future, recognising potential market developments and the impact of recent changes in legislation such as the Data (Use and Access) Act.²⁸
- 3.5 Figure 1 sets out a summary of our assessment of highly effective age assurance methods at 16 and 18. For our preliminary view on the role of age inference in implementing the new age restrictions, see paragraphs 3.64 to 3.68.

²⁷ Ofcom, 2025. [Guidance on highly effective age assurance for Part 3 services](#), pp.8-9.

²⁸ Section 45 of the Data (Use and Access) Act 2025 contains a power that is referred to as the "information gateway", which allows public authorities to share information with digital verification service providers, as long as information meets certain provisions. Office for Digital Identities and Attributes (OfDIA), 2026. [The information gateway: enabling secure sharing of information held by public authorities with trusted digital verification services – Enabling digital identity](#). [accessed 28 September 2026].

Figure 1: Age assurance methods we have assessed



What kinds of age assurance are capable of being highly effective at determining whether a user is 16 or over?

Photo ID matching

- 3.6 **How the method works:** Photo ID matching works by checking relevant information on a photo ID document and comparing the photograph on the document to an image of the user captured during the age check. This helps verify that the photo ID belongs to the user completing the check.
- 3.7 **Circumvention risks and mitigations:** Potential circumvention methods for photo ID matching include the use of borrowed or stolen identity documents, forged or synthetic documents, and situations where a parent knowingly provides identification for a child to use. These circumvention techniques can be mitigated by authenticity checks of IDs and selfie matching with liveness detection.²⁹
- 3.8 **Accessibility:** Photo ID matching requires users to have independent access to an accepted identity document with a photo, and for them to be able to complete a document and facial image capture process using a suitable device.³⁰ We discuss the uptake and accessibility of photo IDs in paragraphs 3.32 to 3.39.
- 3.9 **Privacy considerations:** This method involves the processing of identity attributes such as a date of birth and potentially involves the processing of special category biometric data to

²⁹ Ofcom, 2025. [January 2025 Statement](#), paragraph 3.83,

³⁰ OfDIA has produced guidance on how a service can reach a particular level of confidence when checking someone's identity, including when to use an authoritative source. See OfDIA, 2026. [How to check someone's identity](#). [accessed 8 October 2026].

undertake the matching process.³¹ The privacy impacts will depend on factors including whether or not data is retained, the amount of personal data available on the identifier, and whether this is done through a third-party provider. For example, where a service provider chooses to use a third-party age assurance provider, the information shared during the age check could be limited to a confirmation of whether a user is above or below a certain age (a 'yes' or 'no' response). This could limit the amount of sharing other identifying information shared about the user. Privacy considerations are not a barrier to use of this method, as long as data protection law and ICO guidance is followed.

Digital identity services

- 3.10 **How the method works:** Digital identity services enable people to digitally prove who they are (identity) or information about themselves (attributes). There are 275 firms currently providing digital identity products and services in the UK.³² Reusable digital identities or attributes can be used multiple times for different interactions and transactions, for example, through the use of digital identity wallets which enable users to securely store attributes, such as age, in a digital format. Once an identity or attribute has been verified, a user may choose to share attributes such as their age or age range with the service requesting it. As of September 2026, approved digital proof of age can be legally accepted when buying alcohol in England and Wales.³³
- 3.11 The UK Digital Verification Services Trust Framework, overseen by the Office for Digital Identities and Attributes (OfDIA), sets out the rules and standards for the provision of trusted digital verification services across the UK and maintains a list of trusted providers.³⁴ Using a digital identity service certified against the trust framework could help a service provider evidence that it has met the four criteria needed for a method to be considered highly effective.³⁵ OfDIA have committed to exploring the role that trusted digital verification service providers could play in supporting highly effective age assurance for an under-16 social media ban.³⁶
- 3.12 **Circumvention risks and mitigations:** The reliability of this method will depend on the underlying process used to verify a user's age. There is also a risk of a child using another person's digital identity to complete a check. Services could mitigate this through using secondary biometric or authentication checks.
- 3.13 **Accessibility:** To prove an individual's identity or specific attributes, digital identity services will likely need to verify a user's age by checking information from an authoritative source. As a result, digital identity services are currently unlikely to be available to 16- and 17-year-

³¹ The ICO have produced [biometric data guidance](#) on processing this particular kind of attribute [accessed 1 October 2026].

³² OfDIA, 2026. [Digital Identity Sectoral Analysis Report 2026](#). [accessed 8 October 2026].

³³ OfDIA, 2026. [New rules pave the way for businesses to adopt digital proof of age for alcohol sales - GOV.UK](#). [accessed 8 October 2026].

³⁴ OfDIA, 2024. [Digital verification services register](#). [accessed 26 August 2026].

³⁵ Our existing HEAA guidance explains that using a service certified against the Digital Verification Services Trust Framework (or any other standard or scheme) is not an automatic means of compliance with existing regulations and we expect this will be the case for future guidance. Ofcom, 2025. Guidance on highly effective age assurance, p.12.

³⁶ OfDIA, 2026. [Office for Digital Identities and Attributes annual report on the operation of Part 2 of Data \(Use and Access\) Act 2025](#), p.26. [accessed 27 August 2026].

olds who do not have access to a photo ID.³⁷ However, for users who do have a photo ID document, the use of a digital identity service will reduce the need to repeatedly access it to prove their age, reducing user friction.

- 3.14 **Privacy considerations:** A digital identity service gives users the option to select which attributes to share with a related service completing the age check. For example, a user could share only their age or age range with a service, without the accompanying personal and biometrics data commonly included in a photo ID document. When only an age range, such as '16 and above' is shared, this limits the amount of information that users share with the regulated service provider. However, regardless of the amount of information shared, regulated service providers will have to meet their data protection obligations.

Banking information

- 3.15 **How the method works:** Banking information works by accessing the information a bank or other financial institution has on record regarding a user's age, with the user's consent. This may involve the user accessing the information from their bank or financial institution themselves or via a third-party age assurance provider. Confirmation of the user's age, age range, or date of birth can be shared with the service requesting it.³⁸
- 3.16 **Circumvention risks and mitigations:** Due to existing security infrastructure and financial regulations, banking methods can be considered robust against circumvention attempts, however, regulated service providers would still need to ensure the method fulfilled the robustness criterion.³⁹
- 3.17 **Accessibility:** As with digital identity services, users would typically need to provide an identity document or other trusted evidence of identity to open an account, but once opened, this may provide a more convenient user experience. According to data from the Money and Pensions Service's 2022 Children and Young People's Financial Wellbeing Survey, around 90% of UK 16- to 17-year-olds held a bank account.⁴⁰
- 3.18 The ability of these users to complete a banking-based age assurance check will also depend on the reach of the banks participating in or developing bank-based age assurance solutions at the time any regulations are introduced. We are aware of some early-stage solutions that include major banks which could be capable of offering age assurance checks by the time any regulations come into force.⁴¹

³⁷ There may be other ways for a digital identity service to verify a user. See OfDIA, 2026. How to check someone's identity.

³⁸ This method differs from the open banking solution we set out in our existing HEAA guidance. Though open banking solutions could in theory be used to determine whether a user is 16 or over, its practical application is currently limited because the approach relies on age-specific bank accounts, which are not widely offered at age 16 and above. Therefore, we have adopted a wider definition to account for other ways information could be shared. Age verification through online payment methods which do not require a user to be over age 16 cannot be used as a method of highly effective age assurance at 16. Ofcom, 2025. Guidance on highly effective age assurance, p.8.

³⁹ Age Verification Provides Association (AVPA), 2026. [Age Assurance at 16 White Paper](#), pp.26-27.

⁴⁰ Money and Pensions Service (MaPS) Children and Young People's Financial Wellbeing Survey, 2022. Estimate based on approximately 800 interviews with UK 16- to 17-year-olds and includes current and savings account, as well as those who did know which type of account they had. The figure was provided and verified by MaPS for publication in this assessment.

⁴¹ From our engagement with one age assurance provider [X] working with several high street banks and another bank [X] developing a proprietary solution.

- 3.19 **Privacy considerations:** As with other methods offered by third parties, it is possible to limit the information shared to a confirmation of whether a user is over a certain age, thereby limiting the amount of personal information shared with the regulated service. The privacy implications would depend on how the method is implemented.

Facial age estimation

- 3.20 **How the method works:** Facial age estimation works by analysing the features of a user's face to estimate their age or age range. This may be more accessible than other methods because users can typically complete the process without needing to provide a photo ID document or share other personal information.
- 3.21 **Technical accuracy:** Results from accuracy testing conducted by the US National Institute of Standards and Technology (NIST) shows that the performance of facial age estimation for the 13 to 17 age group is comparable to its performance for adults.⁴² A common measurement of assessing a facial age estimation's algorithm's performance at estimating particular ages or age ranges is mean absolute error (MAE).⁴³ Using NIST's data, it is possible to compare the MAE for models designed to determine an age required by an age gate of 16 and 18. NIST results shows that, for most algorithms, MAE increases with age, with comparable performance across the two key age groups for a 16 and 18 age gate.
- 3.22 For the 13 to 17 age group, the lowest MAE is 1.77 years. Nineteen out of 50 algorithms tested have a MAE below 3 years for this age group. For the 18 to 25 age group, the lowest MAE is 2.39 years. Nine out of the 50 algorithms tested have a MAE below 3 years for this age group.⁴⁴ This means that some facial age estimation technologies can accurately determine the age of users above and below 16 with a margin of error of a few years.
- 3.23 The margin of error for facial age estimation becomes more significant for the ages closest to the target age gate (16 in this case). For example, if the facial age estimation algorithm is accurate within two years for children aged 15, it could estimate them as aged 17. This could result in significant numbers of children under 16 gaining access to services or functionalities that are restricted. It could also result in a 17-year-old being denied access if they are estimated to be 15, unless they use another method. However, this is only likely to affect users who are close to the target age, as most adults offered this method would be estimated to be clearly above 16.
- 3.24 In order to account for the margin of error in a facial age estimation algorithm, services should implement a 'challenge age' (sometimes known as a 'buffer age'). A challenge age approach is widely used in an offline context when selling age-restricted products like alcohol in retail environments, for instance, through the retailing strategy 'Challenge 25.' In this approach, anyone who appears to the provider of restricted products to be under the

⁴² There are several organisations who conduct testing on facial age estimation, and several metrics which can be assessed. The most well-known organisation conducting testing is the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce. NIST's Face Analysis Technology Evaluation: Age Estimation and Verification open programme allows companies providing facial age estimation products to submit their algorithms for testing, with the results published in reports available on the NIST website. NIST, 2024. [Face Analysis Technology Evaluation: Age Estimation and Verification](#). [accessed 7 September 2026].

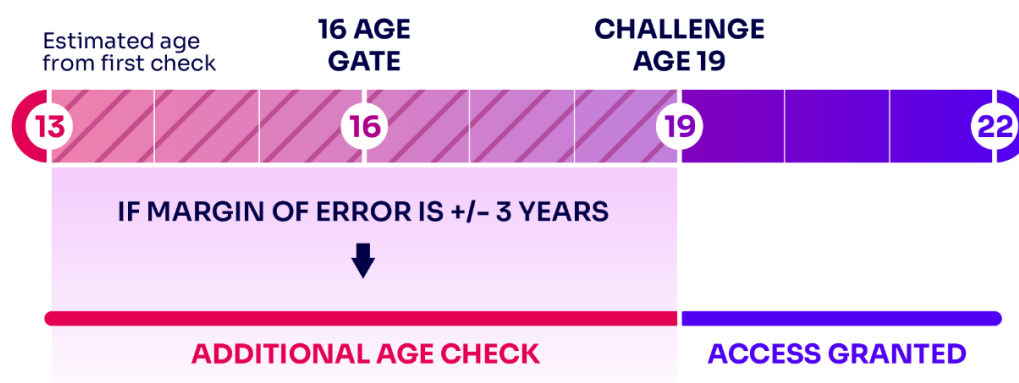
⁴³ Mean absolute error is the central value of the absolute error. It describes the average discrepancy between a user's technology determined age and their actual age, ignoring whether it is an over- or under-estimation.

⁴⁴ NIST, 2024. Face Analysis Technology Evaluation.

age of 25 should be challenged to provide acceptable ID proving that they are over the age of 18 if they wish to buy alcohol.

- 3.25 The use of a challenge age for facial age estimation would be necessary to reduce the number of users who are under 16 from gaining access to restricted service or functionalities. We would expect services to set a challenge age at an appropriate level according to the margin of error of the particular technology being used. This is consistent with our recommendations for any age estimation method.⁴⁵
- 3.26 While most adult users would likely be estimated to be above the challenge age, those close to the target age (16 in this case) would be more likely to be asked to provide additional proof of age.⁴⁶ For example, if the challenge age was set at 19, users estimated to be between 16 and 19 years old would likely need to undergo an additional age check.⁴⁷ This is shown in Figure 2.

Figure 2: Illustration of a how a challenge age may work in practice.



- 3.27 **Circumvention risks and mitigations:** Users may attempt to circumvent facial age estimation checks by using a photograph, video, or any other form of spoofed representation of an older person. As with other methods, liveness detection can help to ensure that children are not using images of adults to pass through checks. The risk that users may attempt to deliberately appear older through simple tricks should be accounted for in testing.⁴⁸ Retry limits may also help to reduce circumvention risks associated with facial age estimation.⁴⁹

⁴⁵ Ofcom, 2025. Guidance on highly effective age assurance, p.13.

⁴⁶ A 16- or 17-year-old could be estimated as over the challenge age and therefore not require an additional check. The challenge age is in place to prevent users who are under 16 from being estimated as over 16.

⁴⁷ Provider [X] submitted performance data to Ofcom of a facial age estimation solution designed for the 16 age gate. It indicated that false positives rates (in this case where an individual is estimated to be over 16 when they are under 16) significantly decreased with the implementation of a challenge age to varying degrees, depending on the challenge age set (the higher the challenge age, the fewer false positives, particularly for those age 15).

⁴⁸ A survey conducted between September and October in 2025 found that 3% of children used a random photo to pass facial age estimation checks in the past 2 months and focus groups mentioned young people drawing facial hair on themselves as a method of bypassing age check. Internet Matters, 2026. [The Online Safety Act: Are children safer online?](#), pp.15-16.

⁴⁹ AVPA, 2026. Age Assurance at 16 White Paper, p.22.

- 3.28 **Privacy considerations:** As with photo ID matching, facial age estimation may include the processing of special category biometric data and privacy implications will depend on how the method is implemented.⁵⁰

Can these methods work effectively for all users?

What are the accessibility and inclusion considerations for age assurance at 16?

- 3.29 Age assurance methods can exclude users at any age if they rely on processes that are not accessible and inclusive to everyone.⁵¹ The nature and extent of these impacts may vary depending on the age assurance method used, and may affect some groups differently, including those that share protected characteristics identified in equalities legislation.⁵² For example, some methods may be less accurate for certain groups if they are not tested on diverse population data and do not meet our fairness criterion.⁵³
- 3.30 When considering age assurance at 16, we expect 16- and 17-year-olds may be particularly impacted by accessibility and inclusion considerations. These impacts arise because there are currently fewer highly effective methods available for this age group.
- 3.31 Users with special educational needs and disabilities may encounter more barriers, particularly where age assurance processes are more complex and contain multiple steps. Other users may be unable to complete checks that involve facial scanning unless they have access to a smartphone or tablet with a working camera. This is more relevant to younger users aged 16 and 17 than those over 18 as there are fewer methods available that are considered 'easy to use' and do not rely on such technologies (such as email and mobile-based methods).
- 3.32 Methods that require a photo ID document can exclude users at any age if they do not possess one.⁵⁴ For example, age assurance methods which rely on the use of photo ID documents may have a greater negative impact for users from disadvantaged backgrounds, who are statistically less likely to have a passport.⁵⁵ Evidence suggests that young people in the care system and particularly those in short term placements could be less likely to have a form of photo ID.⁵⁶
- 3.33 Our preliminary assessment suggests that 16- and 17-year-olds are more likely than users of other ages to need access to a photo ID document. Of the methods listed as capable of being highly effective at 16, a photo ID will likely be needed at some point in the process. This is either because the method itself requires a photo ID, because ownership of a photo ID is part of the underlying process for accessing another method (such as opening a bank account or using a digital identity service), or because a 16- or 17-year-old will most likely

⁵⁰ See ICO [biometric data guidance](#).

⁵¹ A non-exhaustive list of the ways age assurance can exclude certain groups can be found here: AVPA, 2023. [Design Age Assurance for Accessibility and Inclusivity](#) [accessed 9 September 2026]

⁵² There may also be obligations for service providers under the Equality Act 2010. Guidance on this can be found at [Equality and Human Rights Commission Guidance](#). [accessed 15 September 2026].

⁵³ This is particularly relevant for methods that involve the processing of biometric data that should account for different skin tones, genders and atypical facial features.

⁵⁴ Cabinet Office, 2021. [Photographic ID Research: Headline Findings Report](#). [accessed 28 September 2026].

⁵⁵ In England, 21.2% of those in the most deprived areas do not have a passport compared to 7.1% in the least deprived. From [English Census data on passport ownership, 2021](#) layered with [English indices of deprivation 2025](#). [accessed 28 September 2026].

⁵⁶ Praesidio safeguarding, DCMS. 2023. [Making age assurance work for everyone: inclusion considerations for age assurance and children](#), p.4.

fall within the challenge or buffer age for facial estimation methods and be asked to prove their age with a secondary method.

Current uptake figures of passports and (provisional) driving licences

- 3.34 An estimated 94% of people aged 16 and over in the UK have either a passport or driving licence.⁵⁷ As 16- and 17-year-olds are more likely to need access to a photo ID, we have provided a breakdown of current uptake figures of passports and driving licences for these ages in Table 3.

Table 3: Estimated uptake of passports and driving licences for those aged 16 and 17⁵⁸

Photo ID document	16-year-olds	17-year-olds
Passport Ownership Based on 2021/2022 UK-wide Census data	89%	89%
(Provisional) driving licence ownership Based on driving licences issued in Great Britain as of August 2026. ⁵⁹	19%	65%

- 3.35 These percentages should be interpreted as a current snapshot of document ownership, rather than the proportion of young people who are able to obtain one. Differences in uptake may reflect the relative usefulness of each form of photo ID for each age group. For example, while it is possible to apply for a UK provisional driving licence from the age of 15 years and 9 months, there are limited reasons for doing so until a young person is preparing to learn to drive at age 17 or purchase alcohol at aged 18, especially when there is an associated cost with obtaining a licence. While we do not know the exact number of young people who have neither a passport nor (provisional) driving licence, evidence provided to us by CitizenCard suggests that around 150,000 16- and 17-year-olds across the UK hold neither.⁶⁰

What other forms of photo ID could be used?

- 3.36 Sixteen and 17-year-olds without access to a passport or (provisional) driving licence will most likely need to take active steps to obtain one, or obtain another form of photo ID. One alternative is to apply for a photo ID card certified by the Proof of Age Standards Scheme (PASS).⁶¹ There are multiple PASS-accredited providers and the application process varies

⁵⁷ This includes provisional driving licences. Electoral Commission, 2026. [Public attitudes to elections and democracy: winter tracker](#). [accessed 14 October 2026].

⁵⁸ Passport ownership based on 2021/2022 Census data ([England and Wales](#), [Scotland](#), [Northern Ireland](#)). [accessed 9 September 2026]. Please note that for Scotland combined numbers for 16- and 17-year-olds were used. Driving licence data based on August 2026 [Department of Transport GB Driving Licence Data](#) and Office for National Statistics (ONS) [Mid-2025 estimates of the population for the UK, England, Wales, Scotland, and Northern Ireland](#). [accessed 1 October 2026].

⁵⁹ Driving licence estimates do not include Northern Ireland.

⁶⁰ Estimated from a non-representative sample survey conducted in schools with 8,459 respondents aged 16 and 17. It is possible to apply for a (provisional) driving licence without a passport.

⁶¹ The Proof of Age Standards Scheme (PASS) is the UK's national proof of age accreditation scheme, endorsed by the Home Office, the National Police Chiefs' Council (NPCC) and the Security Industry Authority (SIA). The list of PASS schemes and suppliers can be found on the [PASS Scheme website](#). [accessed 14 October 2026].

by provider, however in many cases, it is possible for 16- and 17-year-olds to apply for a PASS-accredited card without holding an existing photo ID document.

- 3.37 The Young Scot National Entitlement Card is a free, PASS-accredited card available to 11 to 26 year olds living in Scotland that can be applied for without an existing photo ID document and already has widespread uptake.⁶² This means that 16 and 17-year-olds in England, Wales and Northern Ireland are more likely than those Scotland to need to obtain a photo ID if they do not have access to a passport or (provisional) driving licence, as they are less likely to already have a PASS-accredited card.
- 3.38 Since 1 October 2026, CitizenCard has offered their PASS-accredited photo ID card to 16- and 17-year-olds in the UK for free. The cost of the card has been removed to facilitate the accessibility of proof of age ID in support of the social media ban announcement.⁶³ This means that there will not be an additional cost burden on 16- and 17-year olds outside of Scotland to obtain photo ID when the regulations come into force. It is also worth noting that over 50% of applications for a 16- to 17-year-old CitizenCard card were completed without another form of photo ID at sign up and a passport or licence does not need to be obtained before applying.⁶⁴

What are the barriers to obtaining photo ID?

- 3.39 Despite free options being available, there are potential barriers to accessing any type of photo ID document. Some 16- and 17-year-olds may need support during the application process and therefore would need access to a willing parent, guardian, or professional. Others may already have a photo ID document but might not have independent access to it if it is held by an adult (for example, when a passport is kept in a family safe) meaning they may still need to seek permission to complete an age check despite being over 16.⁶⁵

What are the key considerations for services when implementing the new restrictions?

- 3.40 The introduction of restrictions for under-16s and safety defaults for 16- and 17-year-olds, alongside existing measures for the protection of all children under 18, means that some providers (those in scope of regulation for both under-16s and under-18s) may need to operate age assurance processes at both ages. This would present some implementation choices for those service providers.⁶⁶
- 3.41 For service providers who are required to implement highly effective age assurance at 16 and 18, or are required to offer one or more safety defaults to 16- and 17-year-olds, a precise age check may be helpful. This would likely be through using an age verification method, which would confirm a user's age against a date of birth at some point in the

⁶² This is based on 64,739 cards being issued to 16-year-olds and 67,076 being issued to 17-year-olds in Scotland as of June 2026. This widespread uptake may be due to the fact that the card offers access to discounted or free public transport.

⁶³ CitizenCard. [Free photo ID for more young people: the 16-17 CitizenCard online offer](#). [accessed 1 October 2026].

⁶⁴ This is based on 36,686 16- and 17-year-old card holders as of September 2026. Cards can be obtained through a trusted referee or school programme.

⁶⁵ Praesidio safeguarding, DCMS, 2023. Making age assurance work for everyone, p.5.

⁶⁶ We do not yet know which services will be in scope of both the announced restrictions for under-16s and under-18s.

process. Examples include photo ID matching, banking information or digital identity services.

- 3.42 Age estimation methods alone do not process a date of birth and may not be able to accurately place a user in the 16 to 17 age range with enough precision to operate dual age restrictions. As set out in our existing HEAA guidance, services using an age estimation method should use a challenge age, which would likely need to be over 18 for the 16 age gate, meaning 16- to 17-year-olds would likely need to prove their age using age verification.
- 3.43 If providers decide to ‘age up’ accounts automatically to enable users to move through different age groups as they age, they will need to obtain and retain a user’s date of birth. There are potential trade-offs for services to consider when deciding whether to take this approach: users would either need to consent to having their date of birth processed in this way; or complete a second age check at 18 to access an unrestricted version of a service, which may increase user friction and have additional costs.

What additional age assurance methods are capable of being highly effective at 18?

- 3.44 Our preliminary assessment suggests that the methods in this section are not capable of being highly effective at determining whether a user is 16 or over but are capable of determining whether a user is 18 or over. These methods could therefore form part of a service provider’s wider approach to age assurance, offering adults more choice in how they prove their age. This is because a user determined to be 18 or over through a highly effective age check would not need to complete a further check to prove they are over 16.
- 3.45 Not all of these methods require a photo ID and therefore processes may be more accessible overall. They are also generally less intrusive than methods that require users to submit photo ID documents and may offer a more seamless user experience when details are already held by the service, such as an email address or phone number.

Credit card verification checks

- 3.46 Credit card-based age checks work by asking a user to input their credit card details, after which a payment processor sends a request to check the card is valid by the issuing bank. Approval by the issuing bank can be taken as evidence that the user is over 18.
- 3.47 This method cannot be used to determine whether someone is 16 or over as individuals must be 18 or over to obtain a credit card in the UK.⁶⁷
- 3.48 As set out in our existing HEAA guidance, where services implement age assurance processes that rely on details obtained via a user’s identification documents, including credit cards, we would expect providers to have means of checking that the details supplied belong to the user attempting to access the service.⁶⁸

⁶⁷ We are aware that in the US, the term ‘credit card’ can be used to refer to debit cards. For clarity, when we refer to ‘credit card’ we mean cards tied to an account where money is borrowed and repaid, and not debit cards tied to current or ‘checking’ accounts, which often do not have the same 18 and over requirements.

⁶⁸ Ofcom, 2025. Guidance on highly effective age assurance, p.15.

Mobile network operator verification checks

- 3.49 Each of the UK's mobile network operators have agreed to a code of practice whereby they automatically apply a content restriction filter, which prevents children from accessing age-restricted websites over mobile internet on pay-as-you-go and contract SIMs.⁶⁹ Users can remove this filter by proving they are an adult.⁷⁰ Mobile network operator age checks can operate by checking whether the filter on a user's mobile phone has been removed. If the filter has been removed, this indicates that the recorded user of the device is over 18. However, a content filter does not currently exist at age 16.
- 3.50 Other age checks work by retaining information on the account holder, which can include identity information, such as age. This would work in a similar way to banking information.⁷¹ However, individuals under 18 cannot take out a standard pay-monthly phone contract in their own name as it is classified as a credit agreement. and other mobile plans cannot bind the contract holder to the end user of the device.⁷²

Email-based age estimation

- 3.51 Email-based age estimation determines the age of a user by analysing the other online services where that user's email has been used. Many of the strongest signals used by these systems are derived from services that are generally only accessed by adults, such as financial institutions, including mortgage lenders. As a result, we consider this method is not currently capable of reliably determining whether a user is 16 or 17 with sufficient accuracy.
- 3.52 This is the same for mobile number-based estimation methods, which work on a similar principle based on services associated with a phone number.

What age assurance methods are not capable of being highly effective at any age?

Self-declaration of age

- 3.53 This includes asking a user to input their date of birth without any further evidence to confirm this information, or asking a user to tick a box to confirm that they are above a certain age.⁷³
- 3.54 As set out in the Act, self-declaration alone is not considered age verification or age estimation and therefore cannot be used as age assurance for determining if a user is an adult.⁷⁴ For the same reason, we do not consider it would be a highly effective method for determining whether someone is 16 or over.

⁶⁹ Ofcom, 2025. Guidance on highly effective age assurance, p.8.

⁷⁰ There are several ways to remove a content restriction filter, such as by completing a highly effective age check directly with the mobile network operator.

⁷¹ Camara. [Know Your Customer Age Verification – Camara Project](#). [accessed 27 August 2026].

⁷² Based on our engagement with a service provider of a mobile network operator age check solution [3<]

⁷³ Ofcom, 2025. Guidance on highly effective age assurance, p.9.

⁷⁴ Section 230(4) of the Act.

General contractual restrictions on the use of regulated services

- 3.55 This includes restrictions as part of a service provider's terms of service, or general disclaimers asserting that all users should be a certain age or over, without any additional age assurance.⁷⁵ As with self-declaration, this is not highly effective age assurance.

Verifiable parental consent

- 3.56 Verifiable parental consent is where a parent or guardian undergoes an age check to approve a child's access to a platform. While methods for obtaining verifiable parental consent vary, they typically involve a child self-declaring their age and providing an adult's email address.⁷⁶ The adult is invited to undergo an age check themselves to prove they are an adult and then asked to approve the child's self-declared age.
- 3.57 Currently, verifiable parental consent is deployed primarily as a means of obtaining parental consent for the purpose of processing personal data for users under 13 years old,⁷⁷ and to give parents the option of using parental controls, rather than to determine if a user is above or below a certain age.
- 3.58 In our [April 2025 Statement](#) we said we were not aware that verifiable parental consent was being used as a form of age assurance and did not therefore include it in our guidance as a method that is capable of being highly effective. Because the method does not independently verify that the adult providing the consent is related to the child, there is limited assurance that the individual knows the user's age or is accurately representing it. We therefore explained that in considering the potential applicability of verifiable parental consent as a method of age assurance, service providers need to be able to ensure that the email supplied by the child is indeed that of the child's parent or carer.⁷⁸
- 3.59 We have considered this method further in the context of preventing under-16s from accessing a social media service. Even if the relationship between the child and the parent or carer could be verified, there is evidence to suggest that some parents may provide incorrect age information for the purpose of assisting children to circumvent age restrictions.⁷⁹ We therefore do not consider that verifiable parental consent in its current form is sufficiently robust to be considered a highly effective age assurance method at 16.

What new and emerging methods could support new age restrictions for online services in future?

- 3.60 The online age assurance industry is developing rapidly. We expect to see further innovation in methods as the regulatory demand increases and the incentives grow for age

⁷⁵ Ofcom, 2025. Guidance on highly effective age assurance, p.9.

⁷⁶ As VPC does not verify the child's relationship with the parent or carer, all references to 'parental' involvement should be taken to mean the parent, carer or the assigned adult.

⁷⁷ This only applies where a service relies on consent as its lawful basis for processing a child's data.

⁷⁸ Ofcom, 2025. Statement: Protecting children from harms online, paragraphs 13.381 to 13.382.

⁷⁹ ICO and Ofcom evidence suggests that adults help children to circumvent age restrictions. ICO, 2026. [Children's and Parents' Attitudes on Information Rights](#), p.31. Ofcom, 2026. [Adults' Media Lives: Wave 21](#), p.44.

assurance providers and social media service providers to offer users the best experience when proving their age.

- 3.61 At this stage, from our engagement with relevant industry stakeholders we have found limited evidence of new and emerging methods that could be capable in the future of being highly effective at determining whether or not a user is 16 or over.
- 3.62 However, we note that under the “information gateway” in the Data (Use and Access) Act 2025, certified digital verification services can ask for information from public authorities for the purpose of providing a verification service, at the request of the individual to whom the data relates and in compliance with data protection and other legislation.⁸⁰
- 3.63 We anticipate that in the longer term through collaboration and innovation across the industry and beyond, including between digital identity providers, the ICO, OfDIA, Ofcom and the UK Government, this gateway may provide more public information and support new means of determining age. However, this would take time to develop and reach market readiness and is unlikely to support new methods by spring 2027.

What role could age inference play in implementing age restrictions?

- 3.64 As set out in our age assurance report, some social media services currently use age inference models as part of their age assurance approach to detect and apply protections to child users, including in some circumstances to attempt to differentiate between children of different ages.⁸¹
- 3.65 As part of this approach, users are often required to declare their age when first accessing a service. Providers then use a range of statistical or machine-learning age prediction models to infer the user’s age on an ongoing basis. This is often based on ‘signals’ from user behaviour or user interactions with content or functionalities on a service, requiring the processing of personal data.
- 3.66 In our age assurance report, we were clear that current age inference methods cannot act as an age gate, as they require the user to be already interacting with the service.⁸² In the context of preventing under-16s from creating an account or accessing certain functionalities on social media services, we do not consider it would be feasible for services to implement age inference approaches to determine the age of new users. Users are required to be active on the service for a period of time before an inference can be made. Therefore, users, including those potentially under 16, would need to access the restricted service and interact with content and functionalities before they can be determined to be under 16, risking them being exposed to harm.
- 3.67 Age inference models may play a complementary role as part of a wider age assurance system, for instance, in increasing robustness by acting as an anti-circumvention tool to detect under-16s who may have circumvented a highly effective age check.

⁸⁰ For more details see OfDIA, 2026, [‘The information gateway: enabling secure sharing of information held by public authorities with trusted digital verification services’](#). [accessed 9 September 2026].

⁸¹ Ofcom, 2026. [Report on the use of age assurance](#), section 5.

⁸² Ofcom, 2026. Report on the use of age assurance, paragraph 5.30.

- 3.68 We intend to provide more details for service providers in guidance to assist them in implementing highly effective age assurance at 16 to comply with their duties, which we will consult on once the government's draft regulations are laid in Parliament.

4. How could age assurance processes be strengthened?

Circumvention and displacement

- 4.1 Circumvention and displacement could impact how effective the new restrictions are in protecting children under the age of 16.
- 4.2 As the government has acknowledged, some children will seek to circumvent the new age restrictions.⁸³ Our existing HEAA guidance requires service providers to identify and take appropriate steps to mitigate against methods of circumvention by children, to ensure that their age assurance process is robust.⁸⁴ However, the risk of circumvention cannot be entirely eliminated, and some children will succeed in circumventing or bypassing age checks to gain access to age-restricted social media services or functionalities.
- 4.3 Alternatively, children may move to different online services or activities as a result of the new age restrictions (displacement). The risk posed by displacement depends on the risk of harm associated with the services children migrate to.
- 4.4 Twelve months after the new age restrictions come into force, we intend to publish research on circumvention, in consultation with the ICO. This will support the government in ensuring that the new protections for children are effective in practice.

Current evidence on the circumvention of age assurance measures

- 4.5 Circumvention can occur at different levels of the system and at different stages of an age assurance process. Children may circumvent age checks by using techniques that undermine the legitimacy of the age check itself. These include attempts to deceive a facial age estimation check by using a fake or manipulated photo or video, completing an age check by providing false or fabricated information, or relying on an adult to complete an age check on their behalf.⁸⁵ A user may bypass protections altogether by using VPNs or other similar technologies that mask a user's location given that services may only apply these restrictions to users based in the UK. The use of VPNs in the UK is legal and services are not required to prevent access to their service via the use of VPNs. Users may also bypass the age check by accessing the service through an adult's account.⁸⁶
- 4.6 Early evidence from Australia's eSafety Commissioner on SMMA found that the primary reason children continued to hold social media accounts, despite the age restriction, was due to ineffective implementation of age assurance measures by platforms.⁸⁷ Across age-

⁸³ DSIT, 2026. [June progress statement: letter from DSIT Secretary of State to Ofcom Chair and CEO](#).

⁸⁴ Ofcom, 2025. [Guidance on highly effective age assurance for Part 3 services](#), pp.14-16.

⁸⁵ ICO and Ofcom evidence suggests that adults help children to circumvent age restrictions. ICO, 2026. [Children's and Parents' Attitudes on Information Rights](#), p.31. Ofcom, 2026. [Adults' Media Lives: Wave 21](#), p.44.

⁸⁶ In Ofcom research, adults also highlighted account sharing as a likely circumvention route. One participant said that "they'll just get someone else to log in on their behalf." Ofcom, 2026. [Adults' Media Lives](#), p.44.

⁸⁷ eSafety Commissioner, 2026. [Early days, early insights: Understanding experiences of social media age restrictions at the three-month follow up](#), p.12.

restricted platforms, the main reason children gave for why they still held an age-restricted account was that the platform had not yet asked them to confirm their age (50.2%).⁸⁸ There was some evidence of children taking action to bypass age restrictions by listing their age as 16 or over; parental assistance and virtual private network (VPN) use were less common.⁸⁹ This low rate of circumvention could reflect the reduced incentive to circumvent due to many children having continued access to their social media accounts. These findings should be considered in the context of the Australian regime, which requires service providers to take “reasonable steps” to prevent age-restricted users from having accounts, rather than requiring the use of highly effective age assurance.⁹⁰

- 4.7 In our report on the use of age assurance, we found that the circumvention by children of age checks at 18 appeared low, with a relatively small minority of children doing so. However, in the case of pornography services, the availability of services without highly effective age assurance in place meant that children could access pornographic content without needing to circumvent age gates.⁹¹ In Ofcom’s 2026 [Media Use and Attitudes report](#), 5% of children (aged 13 to 17) told us they had got around parental controls and age checks in the past 12 months. However, self-reported figures may understate the true level of circumvention due to response bias.⁹²
- 4.8 Our research on Children’s Use of VPNs, conducted in August 2026, found that a quarter of children had used a VPN in the previous six months. In terms of using VPNs to bypass age restrictions, [we found that 30% of GB 11–17s had accessed content intended for people older than them in the previous six months](#). Among this group, 12% said they had used a VPN to do so.⁹³ Recent ICO research found that over a third (36%) of children aged 12 and over reported ever using a VPN.⁹⁴

The risks of circumvention for the potential new age restrictions

- 4.9 The implementation of new age restrictions for under-16s raises specific risks and considerations:
- **Increased incentive for under-16s to circumvent restrictions:** Social media forms an integral part of many young people’s everyday life and some of the services where they spend the most time will be restricted.⁹⁵ It is therefore likely that the rates of circumvention by children will rise due to increased incentives and the higher number of age checks. We also expect there to be greater knowledge sharing of circumvention techniques among peer groups.
 - **Evolution of circumvention techniques:** As a result of an increased incentive to circumvent, more sophisticated circumvention techniques may emerge as children

⁸⁸ eSafety Commissioner, 2026. Early days, early insights, p.12.

⁸⁹ eSafety Commissioner, 2026. Early days, early insights, p.12.

⁹⁰ Australian Government Federal Register of Legislation, 2024. [Online Safety Amendment \(Social Media Minimum Age\) Act 2024 - Federal Register of Legislation](#). [accessed 26 August 2026].

⁹¹ Ofcom, 2026. [Report on the use of age assurance](#), pp.61-64.

⁹² Ofcom, 2026. [Children and parents: Media Use and Attitudes Report](#), p.58.

⁹³ Ofcom, 2026. [Children’s use of VPNs](#).

⁹⁴ ICO, 2026. Children’s and Parents’ Attitudes on Information Rights, p.37.

⁹⁵ Ofcom, 2026. [Children’s Online Experiences](#), p.10. TikTok, Snapchat, YouTube, Instagram and Facebook each occurred in the 10 service providers children recalled using most and are some of the services the UK Government has said will be in scope of the ban.

try to find new ways around the restrictions. There may be more account sharing between those who do have access to services and those who do not, and more adult-assisted circumvention.

How could these risks be mitigated?

4.10 In light of this, we have identified potential measures that may help reduce the risk of circumvention by children and support the robustness of age assurance processes at 16. We will revisit these measures as part of our draft guidance on highly effective age assurance at 16. These approaches may vary in their effectiveness, and each has limitations that would need to be considered in the context of the overall age assurance process:

- **Age inference:** age inference may play an anti-circumvention role to detect underage users who may have slipped through a highly effective age gate or be sharing an account with an older user.⁹⁶ For example, age inference models could flag accounts that appear to belong to users under 16 who may have circumvented the initial age check, and these accounts would then be directed to complete an additional highly effective age check. In terms of data protection, the Information Commission are clear that any implementation of age inference for this purpose requires services to take a risk-based approach to ensure that it is necessary, effective and proportionate to the level of risk presented to children and should not be used to make up for a weak or non-existent age gate.⁹⁷
- **Use of existing location-related signals:** location-related signals such as IP address, device and time settings, or GPS information may support anti-circumvention measures by helping detect VPN use or find likely UK users subject to jurisdiction-specific age assurance requirements.⁹⁸ Where location-related signals are obtained through the use of storage and access technologies, user consent is required under the Private and Electronic Communications (EC Directive) Regulations 2003 (PECR).⁹⁹ The potential use of location-related signals as an anti-circumvention measure also requires careful consideration, as VPNs can be shared across multiple devices and given the potential impacts on people legitimately using VPNs as a privacy-preserving measure.
- **User reporting:** this mechanism can provide an additional safeguard by enabling other users to flag accounts under 16. Evidence suggests that account restrictions, removals, and deactivations can improve compliance when reports are implemented

⁹⁶ ICO, 2026. [Children's Code Strategy progress update](#) [accessed 26 August 2026]. The AVPA's Feasibility of Age Assurance at 16 in the UK suggests that strong age assurance systems rely on multiple layers of assurance rather than a single verification method. AVPA, 2026. [Age Assurance at 16 White Paper](#), p.17.

⁹⁷ The ICO states that services should take a risk-based approach to ensure that any age assurance measures remain proportionate to the level of risk presented to children. Please note the ICO call age inference 'Profiling for age assurance'. [ICO. 5. Risk assessment and age assurance](#) [accessed 26 August 2026]. ICO. [Annex: What we've learned about profiling for age assurance](#). [accessed 29 September 2026].

⁹⁸ eSafety's Regulatory Guidance on its Social Media Minimum Age Act notes that some services use geolocation tools for real-time VPN detection. It recommends monitoring signals over time rather than relying on a single indicator. [eSafety. Social Media Minimum Age Regulatory Guidance \(v 16 Sep 2025\)](#), p.10. [accessed 26 August 2026].

⁹⁹ Location-related signals which are obtained through the use of storage and access technologies will engage regulation 6 of the Private and Electronic Communications (EC Directive) Regulations 2003 (PECR) and require user consent under that provision. ICO. [How do the PECR rules relate to the UK GDPR](#). [accessed 29 September 2026].

and used correctly.¹⁰⁰ However, for reporting pathways to be effective they need to be accessible, easy to find, and simple to use. Reporting systems are limited by inaccurate or malicious reports, and resource constraints. Therefore, user reporting may be most effective as one component of a wider age assurance process.

- 4.11 We note that deliberate efforts by services to promote or facilitate circumvention (for example, by directing users to VPNs or other means of bypassing restrictions) may raise compliance concerns. As set out in our existing guidance, service providers should not publish content directing users towards methods of bypassing age assurance processes, such as VPNs, which may facilitate and encourage circumvention by children and as such would be considered a compliance failure.¹⁰¹

What role could other actors in the wider ecosystem play to support new age restrictions?

- 4.12 To strengthen protections and reduce friction on users, there are questions about the role that other actors in the ecosystem could play, including operating systems, devices, and app store providers. Our engagement with service providers has shown that there is strong support from some regulated services for highly effective age checks to be carried out at the app store, device or operating system level as part of a 'layered' approach to age checks.¹⁰² Some stakeholders also supported a greater role for these actors in the ecosystem, while noting that such measures may not be sufficient in all circumstances and should not necessarily replace service-level age assurance. These stakeholders highlighted challenges such as shared devices and access via browsers, which may require complementary service-level measures.¹⁰³
- 4.13 Alongside this rapid assessment, we also published our [statutory report on the use of app stores by children](#) in October 2026.¹⁰⁴ The report shows that app stores are the most common route through which children access many regulated user-to-user services. While the report is focused on app stores, as required by the Act, it identifies some wider considerations relating to the relationship between app stores, regulated services, and other actors in the ecosystem that would need to be taken into account in any future legislation.
- 4.14 Our existing HEAA guidance is neutral as to who carries out the highly effective age assurance solutions or makes the results of an age check available. It is the responsibility of the regulated service provider to ensure that age assurance is implemented in such a way that it is highly effective at determining whether or not a user is under the age required by the regulations. Regulated services may choose to use age assurance solutions offered by third parties that are either integrated into their platform or conducted before users access restricted services, content or functionality. We have developed a [Vet Your Vendor](#)

¹⁰⁰ The AVPA concludes that account removals, restrictions and deactivations could have a substantial effect on compliance. – AVPA. Age Assurance at 16 White Paper, p.29.

¹⁰¹ Ofcom, 2025. Guidance on highly effective age assurance, p.16.

¹⁰² Based on our engagement with several large social media service providers [§].

¹⁰³ Based on our engagement with industry stakeholders [§].

¹⁰⁴ [Ofcom, 2026. Report on the use of app stores by children](#)

resource to support service providers' due diligence conversations with third-party age assurance vendors.¹⁰⁵

- 4.15 The role of age assurance in different parts of the ecosystem has implications for data protection, privacy and competition. It also raises broader questions around governance, accountability and the effectiveness of interventions in delivering child safety outcomes. These considerations are outside of the scope of this report.
- 4.16 We also note that the government has committed to explore primary and secondary legislation options to mandate device-level nudity detection measures.¹⁰⁶ We are working with the government to understand how this will work in practice and interact with existing obligations on services.

¹⁰⁵ Ofcom, 2026. [Vet your vendor: a resource to help service providers conduct due diligence on their age assurance vendors](#). [accessed 15 October 2026].

¹⁰⁶ DCMS, 2026. [UK to have world's strongest online child safety laws as government prepares legislation on nude images](#). [accessed 9 October 2026].

5. Next steps

- 5.1 The UK Government has stated that it intends to lay the first regulations related to service level age restrictions on social media services before Parliament by the end of 2026.¹⁰⁷ We plan to consult on draft guidance for services on highly effective age assurance at 16 in the coming months, following the laying of the draft regulations.
- 5.2 We will continue to monitor emerging market and technological developments as we prepare our draft guidance on highly effective age assurance at 16. We welcome the government's intention, announced in August 2026, to improve the availability of age assurance methods for 16- and 17-year-olds by exploring easier access to secure, privacy preserving ways for people to prove their age online.¹⁰⁸ We also note that the government plans to work with industry to help age assurance technologies continue to progress and improve how accurately they can determine the age or age range of users while protecting personal data.¹⁰⁹
- 5.3 We stand ready to implement any new age restrictions and are continuing with our preparations. We have established strong relationships with international counterparts, including Australia's eSafety Commissioner and other regulators, that enable us to share learning on the design and implementation of age restrictions in different jurisdictions. We will continue to work together as new age restrictions are implemented in the UK and elsewhere.
- 5.4 Following the regulations completing the Parliamentary process and coming into force, we will use our powers to ensure that relevant service providers implement and comply with the requirements. We will continue to engage with industry to monitor implementation, assess compliance and, where necessary, take enforcement action to secure compliance and protect UK users from harms.
- 5.5 In the meantime, providers of services likely to be accessed by children remain subject to the children's safety duties under the Act. As we set out in our open letter to service providers, we will continue to monitor compliance with these existing duties to ensure that children are protected online.¹¹⁰

¹⁰⁷ DSIT, 2026. [Growing up in the online world: progress statement \(June 2026\)](#). [accessed 26 August 2026].

¹⁰⁸ DSIT, 2026. Growing up in the online world.

¹⁰⁹ DSIT, 2026. Growing up in the online world.

¹¹⁰ Ofcom, 2026. [Open letter on reminding services of their duties under the Act](#).

A1. Glossary

Term	Meaning
Accessibility	The ability of a method or process to work for all users.
Age assurance	A collective term for age verification and age estimation as defined in section 230 of the Online Safety Act 2023 (the Act).
Age assurance method	The system or technology that underpins an age assurance process.
Age assurance process	The end-to-end process through which the age assurance method or combination of methods are implemented to determine the age or age range of a user.
Age estimation	Any measure designed to estimate the age or age-range of users of a regulated service. ¹¹¹
Age gate	A point from which access to a service, the creation of an account on a service, or access to a feature, functionality or content on a service should not be allowed, unless a user completes a highly effective age check to determine they are over the minimum required age. For example, an age gate of 16.
Age inference	A broad class of estimation techniques that typically analyses user behavioural data and/or user interactions with content or functionalities on services, often referred to as 'signals', to determine age.
Age verification	Any measure designed to verify the exact age of users of a regulated service. ¹¹²
Challenge age approach	An age assurance process comprised of two stages whereby if, at the end of the first stage of process, the estimated age of a user is found to be below a specified age, further steps are taken to estimate or verify the age of the user before determining whether the user is above a specified age.
Circumvention	Deliberate action(s) taken by a user to obtain access to an age restricted service, functionality, or content, for which they do not meet the applicable age requirement. This can be done in a number of ways including: (a) bypassing or attempting to bypass the age gate altogether, such as by using a virtual private network (VPN); (b) misrepresenting their age; or (c) using another person's credentials.
Displacement	The movement of users from one service to another, for example from services with age assurance to those without it. Also referred to as user migration.

¹¹¹ Age estimation is defined in section 230(3) of the Online Safety Act 2023 (the Act).

¹¹² Age verification is defined in section 230(2) of the Act.

Term	Meaning
Fairness	The extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.
Interoperability	The ability of technological systems to communicate with each other using common and standardised formats.
Liveness detection	A feature used to ensure that the face being analysed is not a photograph, video, or any other form of spoofed representation. The primary goal is to prevent attackers from using static images (print attack) or pre-recorded videos (replay attack) to trick the system into making inaccurate age estimates.
Mean Absolute Error (MAE)	The central value of the absolute error. It describes the average discrepancy between a user's technology-determined age and their actual age, ignoring whether it is an over- or under-estimation. It is calculated by summing the absolute errors for a given number of absolute errors, then dividing this by the number of absolute errors.
Part 3 service	A regulated user-to-user or search service under the Act. ¹¹³
Photo-ID document	A document or trusted data source that can provide a reliable age attribute, such as a passport, provisional driving licence, PASS card, bank information or verified digital identity route
Reliability	The degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.
Robustness	The degree to which an age assurance method can correctly determine the age of a user in actual deployment contexts.
Technical accuracy	The degree to which an age assurance method can correctly determine the age of a user under test lab conditions.

¹¹³ Section 4 of the Act.