

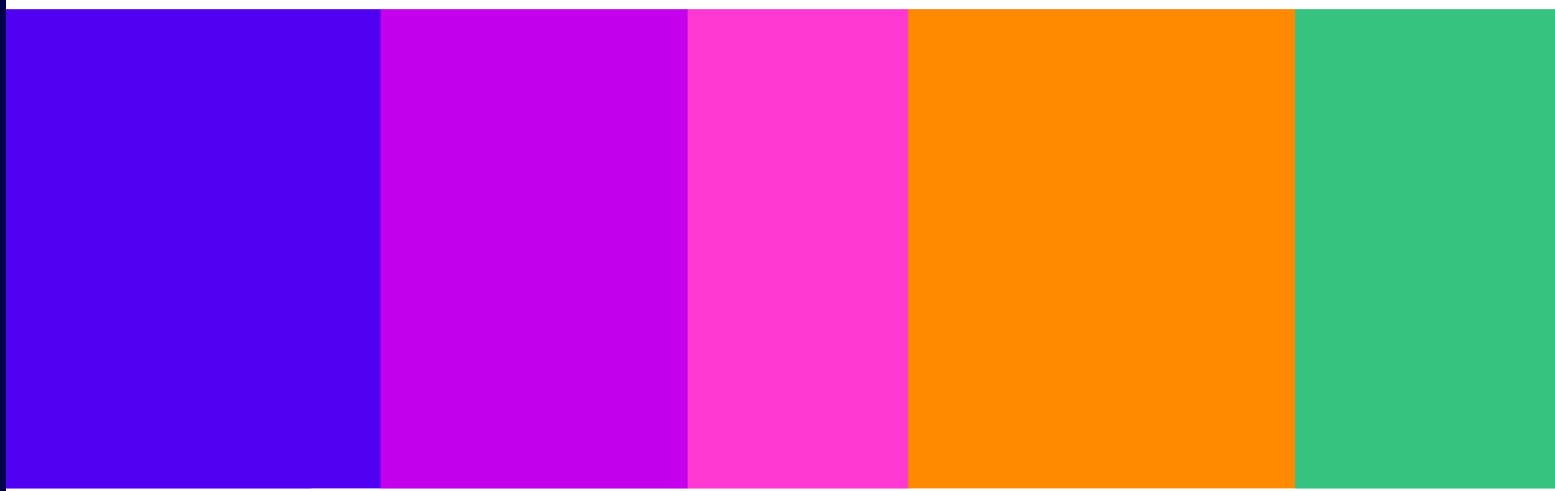
Report on the use of age assurance

Report prepared under s157 of the Online Safety Act 2023

[Welsh version available](#)

Published 15 July 2026

For more information on this publication, please visit ofcom.org.uk



Contents

Section

1. Overview.....	3
2. Introduction, our duties and navigating the report	6
3. Age assurance use and effectiveness across industry	14
4. Pornography services	22
5. Social media services.....	35
6. Dating services.....	45
7. Factors that have prevented or hindered the effective use of age assurance	48
8. Summary of issues and suggested improvements.....	65

Annex

A1. Methodology	68
A2. Detailed analysis of services' regard for highly effective age assurance criteria	74
A3. Cost and choice of age assurance methods	82
A4. Glossary	84

1. Overview

A generational shift towards a more age-aware internet is beginning to take place in the UK, with the rapid adoption of age assurance across a range of services. Ofcom has carried out an assessment of the use and effectiveness of age assurance, based primarily on evidence from the first six months of the protection of children duties being in force. This report lays out early findings across the pornography, social media, and online dating sectors, rather than final conclusions about the effectiveness of age assurance. In line with the duties under the Online Safety Act, Ofcom is sending a copy of this report to the Secretary of State, who will lay it before Parliament.¹

Age checks have increased significantly and are now being deployed at an unprecedented scale. Between July and December 2025, over 69 million age checks were completed across a sample of 32 services operating in the UK and analysed in this report – a 23-fold increase on the previous six months. The true UK total is likely to be materially higher.

Age checks are increasingly shaping children’s online experiences, with more children reporting that they encounter them. Circumvention appears low, although some activity may not be captured due to reporting bias. Many services have implemented age checks in line with our highly effective age assurance guidance (our HEAA guidance), using methods and taking steps to ensure that their age assurance is highly effective in practice.

Highly effective age assurance is helping to prevent children from accessing pornography online. All of the UK’s top 10 and the majority of the top 100 porn sites now have age checks in place. Our research shows that some children are still attempting to access pornography, but in many cases the presence of age assurance appears to deter them.

Despite these positive signs, there is more work to be done to increase the impact of age checks on children’s safety online, across pornography, social media, and online services more broadly. In this report, based on the evidence available and our expertise on age assurance, we outline where regulated services, and other actors in the ecosystem, could go further to protect children online.

Despite the compliance efforts of many pornography services, it is still too easy for children to find services without age checks in place. Many porn sites that have introduced age checks have experienced sharp declines in user traffic, while some sites without age assurance have gained in popularity. Our research shows that almost half of the pornography services visited by children have no age checks in place, and children can find these sites via search engines.

Some of the social media services that children use the most continue to rely on proprietary age inference systems, which we did not include in our HEAA guidance as a method capable of being highly effective. Our analysis indicates variability in performance and reinforces our long-standing, serious doubts about the efficacy of some age inference models, which analyse a user’s activity and behaviour on a platform to estimate whether they are a child or an adult. In some cases, these systems may have failed to correctly identify large numbers of children on their platform, putting them at risk of exposure to harmful content.

Some services have not followed important steps in our HEAA guidance, including the use of liveness detection or a challenge age approach. Where we have identified these issues as a part of our analysis, we have engaged with individual services as a priority on these shortcomings. We urge

¹ Section 157(5) of the Online Safety Act 2023.

all regulated services to ensure they have taken all the necessary steps, as stated in our HEAA guidance, to ensure their age assurance process is highly effective in practice.

Evidence indicates that the direct costs of age assurance are not prohibitively high and are in line with Ofcom's original estimates. However, for many pornography services that have experienced a significant reduction in user traffic this has impacted revenue, particularly where business models rely on advertising to large numbers of users.

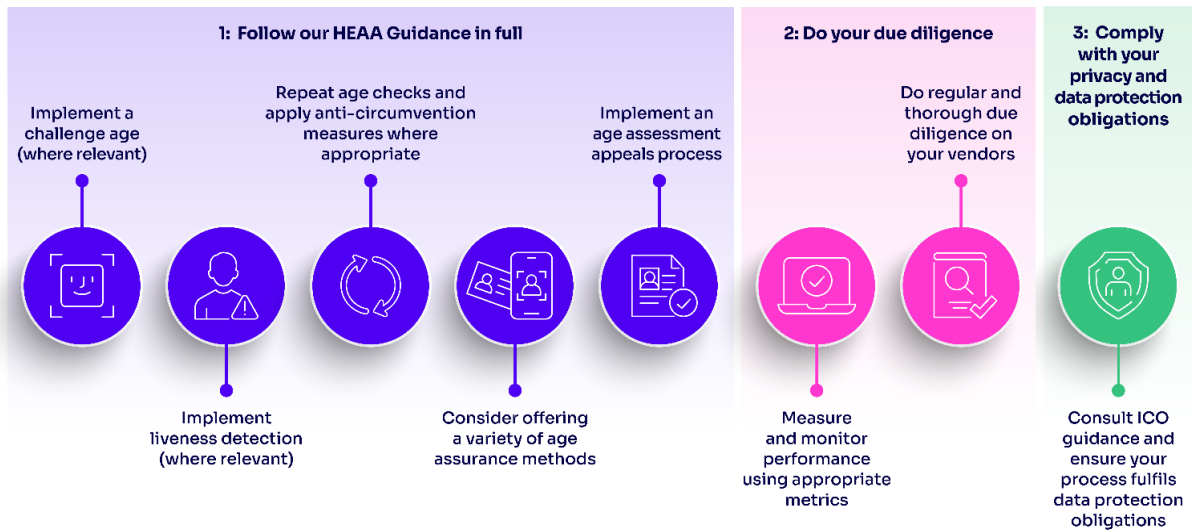
Next steps

Our findings indicate that highly effective age assurance is improving the experience of children online, but more action is needed. While we are clear that the compliance obligations rest on user-to-user services themselves, the protection of children requires a system-wide effort. To strengthen protections and reduce friction on users, there are questions about the role that other actors in the ecosystem can, and should, play, including search engines, operating systems, and app store providers. We welcome innovation in this space, while also emphasising the importance of ensuring that all interventions work effectively and reliably in practice. As a first step, we will consider app-store level protections in our statutory app store report, which we will publish by January 2027.

This report focuses on highly effective age assurance to determine whether a user is over 18, in line with age assurance duties under the Act. We recognise the government's intention to expand age restrictions to prevent under 16s accessing certain social media services. We will deliver to Parliament by the end of October a rapid assessment of what highly effective age assurance looks like for determining whether someone is over 16 to help inform parliamentary debate and in anticipation of potential restrictions coming in 2027.

In the meantime, the existing duties continue to apply.

1. **Pornography services must have highly effective age assurance in place.**
2. **Services with age assurance in place must ensure it is highly effective.** Based on our evidence, we have identified three areas for improvement, shown in the infographic below, that we urge services to implement where relevant:
 - a) Follow our HEAA guidance in full; and
 - b) Conduct regular due diligence on any age assurance vendors you employ, and your age assurance process; and
 - c) Comply with your privacy and data protection obligations.



3. **Services that use age inference should replace or supplement it with other method(s) of age assurance that our HEAA guidance sets out as being capable of being highly effective, unless they can demonstrate using reliable evidence that the way they are deploying these models is highly effective in line with our HEAA guidance, and fulfils UK data protection obligations.**

2. Introduction, our duties and navigating the report

Ofcom's general duties

- 2.1 Ofcom is the UK's independent regulator for communications services, including telecommunications, post, broadcast TV and radio, as well as spectrum, and on-demand programme services. Under the Online Safety Act 2023 (the 'Act'), Ofcom is also the UK regulator for online safety. Under the Act, Ofcom's job is to make online services safer for the people who use them, especially children.

Purpose of this report

- 2.2 This report is produced and published in accordance with section 157 of the Act, to assess:
- a) regulated services'² use of age assurance to comply with their duties in the Act,
 - b) how effective it has been for this purpose, and
 - c) whether there are factors that have prevented or hindered its effectiveness for that purpose.³
- 2.3 The report must, in particular, consider whether the following have prevented or hindered the effective use of age assurance:
- a) the costs to providers of using it, and
 - b) the need to protect users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a regulated service (including, but not limited to, any such provision or rule concerning the processing of personal data).⁴
- 2.4 Section 157 of the Act references the use of age assurance for the purpose of compliance with duties set out in the Act. For the purposes of the Act, a child means a person under the age of 18.⁵ This report therefore focuses on the use of age assurance to determine whether or not a person is 18 or above, as required by the duties explained in paragraphs 2.7-2.15. It does not assess the use of age assurance for the purpose of enforcing a minimum age requirement, either of 13 or 16, for reasons set out in paragraphs 2.17 and 2.19.
- 2.5 In accordance with the Act, this report will be submitted to the Secretary of State, who will lay it before Parliament.⁶
- 2.6 This age assurance report is one of several statutory reports that Ofcom is required to produce under the Act. In the coming months, we will also publish the following:
- a) **Content harmful to children:** A report under section 63 of the Act reviewing the incidence and severity of content harmful to children. This will include advice to the

² Section 4 of the Act.

³ Sections 157(1) of the Act.

⁴ Section 157(2) of the Act.

⁵ Section 236(1) of the Act

⁶ Section 157(5) of the Act.

Secretary of State on whether in Ofcom’s opinion it is appropriate to make changes to the categories of primary priority content and priority content in the Act, specifying any recommended changes.⁷

- b) **App stores:** A report under section 161 of the Act on the use of app stores by children. This will assess the role that app stores play in children encountering harmful content and evaluate the use and effectiveness of age assurance by app store providers.⁸

Legislative and regulatory context

- 2.7 The Act provides a regulatory framework which has the general purpose of making the use of regulated internet services safer for individuals in the UK, seeking to secure a higher standard of protection for children.⁹
- 2.8 Highly effective age assurance is a cornerstone of the Act and critical to the protection of children online. There are several relevant duties in the Act and measures in our [Protection of Children Code of Practice for user-to-user services \(Protection of Children Code\)](#) which require or recommend the use of highly effective age assurance. These duties and measures are outlined below.
- 2.9 Part 5 of the Act imposes specific duties on service providers that display or publish pornographic content on their online services (Part 5 services).¹⁰ Specific duties are imposed on these services to use a form of age assurance that is highly effective at correctly determining whether a particular user is a child, to ensure that children are not normally able to encounter such content on their service along with record keeping duties.¹¹ In order to comply, age assurance must be applied before a user is able to view any pornographic content or access the service, unless the user has been determined to be an adult. In January 2025, these duties came into force and we published the [Guidance on highly effective age assurance and other Part 5 duties \(Part 5 HEAA guidance\)](#).
- 2.10 Under Part 3 of the Act, user-to-user services, including services that may host user-generated content that is pornographic or otherwise harmful to children, and search services (Part 3 services), are required to carry out a children’s access assessment to determine if they are “likely to be accessed by children”. As explained in our [Children’s access assessments guidance](#), we anticipate that most Part 3 services that do not use highly effective age assurance are likely to be accessed by children within the meaning of the Act.
- 2.11 In July 2025, the protection of children duties for user-to-user services likely to be accessed by children, as set out in section 12 of the Act, came into force. These provide that where these services do not prohibit primary priority content (PPC), they must use highly effective age assurance to prevent children from encountering PPC identified on the service.¹² PPC includes pornographic content, as well as suicide, self-harm and eating disorder content.¹³

⁷ Ofcom, 2026. [Call for Evidence: Ofcom's statutory report on content harmful to children](#)

⁸ Ofcom, 2025. [Call for Evidence: Statutory reports on age assurance and app stores](#)

⁹ Section 1 of the Act.

¹⁰ Section 80 of the Act.

¹¹ Section 81 of the Act.

¹² Section 12(4)-(6) of the Act.

¹³ Section 61 of the Act.

- 2.12 In addition, all user-to-user services likely to be accessed by children have a duty to protect children in age groups judged to be at risk of harm from other content that is harmful to children, including priority content (PC) and non-designated content (NDC).¹⁴ PC includes content which is abusive and targets certain characteristics such as race, religion, sex, disability; content which incites hatred against people of a particular race or religion; content which encourages violence against a person; bullying content; and content which encourages or provides instructions for a challenge which is highly likely to result in serious injury to a person.¹⁵ NDC includes any other kind of content that may be harmful to children beyond the kinds specified by the Act.¹⁶
- 2.13 The Protection of Children Code recommends measures providers may take to comply with the duties in section 12 of the Act, including on when and how user-to-user services should use highly effective age assurance to prevent children from encountering PPC and protect them from PC.¹⁷ In summary, the Protection of Children Code recommends user-to-user services likely to be accessed by children use highly effective age assurance to comply with the duties set out in section 12 in the following circumstances:
- a) if a service has a principal purpose of hosting or disseminating one or more kinds of PPC and/or PC, when it should be used to prevent children from accessing the entire service;¹⁸
 - b) if a service does not expressly prohibit one or more kinds of PPC (or prohibits all kinds but they are currently unable to remove it), when it should be used to ensure children are prevented from encountering PPC identified on the service;¹⁹
 - c) if a service does not expressly prohibit one or more kinds of PC for which it is medium or high risk (or prohibits all kinds but they are currently unable to remove it), when it should be used to ensure children are protected from encountering PC on the service;²⁰
 - d) if a service has a content recommender system which is accessible to children and does not prohibit one or more kinds of PPC, PC, or NDC for which it is medium or high risk, when it should be used to apply measures to ensure their content recommender systems protect them from harmful content.²¹
- 2.14 We have published [Guidance on highly effective age assurance for Part 3 services \(Part 3 HEAA guidance\)](#) to assist Part 3 service providers in understanding whether an age assurance process is highly effective and complying with the recommended measures in the Protection of Children Code. We designed both the Part 5 HEAA guidance and Part 3 HEAA guidance to be flexible, technology-neutral and future-proof, with the protection of children at their heart. In both pieces of our HEAA guidance, we included four criteria that age assurance methods must meet to be considered highly effective: technical accuracy,

¹⁴ Section 12(3)(b) of the Act.

¹⁵ Section 62 of the Act.

¹⁶ Section 60(2)(c) of the Act.

¹⁷ Protection of Children Code.

¹⁸ Protection of Children Code, measures PCU B2 and PCU B3.

¹⁹ Protection of Children Code of Practice, measures PCU B4. See also measure C2 which explains the action that should be taken to prevent children from encountering primary priority content (PPC).

²⁰ Protection of Children Code of Practice, measure PCU B5. See also measure C2 which explains the action that should be taken to protect children from encountering priority content (PC).

²¹ Protection of Children Code of Practice, measures PCU B6 and PCU B7. See also measures PCU E1 and PCU E2 which explain the measures Ofcom recommends to secure safer recommender feeds.

robustness, reliability and fairness. We also set out a non-exhaustive list of seven age assurance methods that we consider are capable of being highly effective as well as some methods – including self-declaration of age – that are not capable of being highly effective.

- 2.15 Further details of the duties relating to the protection of children in the Act can be found in the Legal framework in our [April 2025 Statement: Protecting Children from harms online \(our April 2025 Statement\)](#).²²

Matters that are not in scope of this report

- 2.16 We have not considered the use of search services by children for the purposes of this report as the duties which apply to regulated search services are different to those which apply to user-to-user services. In particular, neither the duties in section 29 of the Act or the [Protection of Children Code for search services](#) require the use of highly effective age assurance by regulated search services.
- 2.17 We have not considered the use of age assurance in relation to minimum age limits for the purposes of this report as there is no requirement in the Act to set a minimum age limit or use highly effective age assurance to enforce any minimum age limit services choose to set. Where service providers use age assurance to restrict access to users under a certain age, they must enforce these age limits consistently to ensure children have age-appropriate experiences and are protected from harmful content.²³
- 2.18 We have not considered the use of age assurance by app stores in this report. As stated in paragraph 2.6, we will explore this as part of a separate statutory report that will be published by January 2027.
- 2.19 This report does not consider or address the Government’s announcement to ban under 16s from certain specified internet services. The UK Government announced on 15 June 2026 that it will introduce a ban on certain social media sites and platforms which include high risk features, such as livestreaming and contact with strangers for under 16s. The Secretary of State has the power under section 214A of the Act to make regulations introducing the ban.²⁴ The Government has asked Ofcom to conduct a rapid study on what is effective age assurance for verifying whether someone is over 16 by October 2026. The Government expects the Regulations to be laid before Parliament before the end of 2026 with protections expected to come into force in Spring 2027.

²² See Annex 4 in [Volume 5, Annexes](#).

²³ Section 12(11) of the Act.

²⁴ The Children’s Wellbeing and Schools Act 2026 inserts a new section 214A into the Act which gives the Secretary of State new powers to make regulations requiring providers of specified internet services to prevent or restrict access by children of or under a specified age to those services or to specified functionalities or other features of the service. Further information about the age restrictions for under 16s can be found [here](#).

Overview of methodology

Summary of our overall approach

- 2.20 To produce this report, we have drawn on a combination of sources, including information notices issued to a sample of regulated services, Ofcom research on children's online experiences, third-party data sources and responses to a dedicated Call for Evidence (CfE).²⁵
- 2.21 Most of these sources assess the impact of age assurance in the first six months after the children's safety duties came into force (July 2025 to December 2025).
- 2.22 See Annex A1 for a detailed methodology, including the main evidence sources used in this report, sample information, fieldwork timings, and key limitations.

Information from regulated services

- 2.23 For this report, we used our statutory information gathering powers under the Act to issue information notices to a sample of 32 services that are in scope of age assurance duties under Part 3 or Part 5 of the Act, covering a range of service types and implementation approaches.
- 2.24 In the information notices we asked questions about service providers' approach to age assurance, including their process design, steps taken to ensure effectiveness, monitoring and impact, and costs.
- 2.25 For the purpose of our analysis, we subdivided the 32 services in this sample into three categories:
 - a) **pornography services** (19)²⁶
 - b) **social media services** (9)
 - c) **dating services** (4)
- 2.26 For the purpose of this report, the term 'social media services' covers a broad range of user-to-user services including video sharing and messaging services.²⁷
- 2.27 For social media services, we have further differentiated based on the approach to age assurance that they have implemented, for which we observed two overarching approaches:
 - a) **active age gated content approach**, where the requirement to complete an age check is limited to users attempting to access specific content, functionalities, or parts of the service unsuitable for children; and
 - b) **passive age inference approach**, where services 1) ask users to declare their age and 2) use age prediction models to subsequently infer whether a user is an adult or a child.
- 2.28 Throughout the report, we use the term 'analysed services' to refer to the overall sample.

²⁵ Ofcom, 2025. Call for evidence: Statutory reports on age assurance and app stores.

²⁶ The sample of pornography services included those whose are in scope of Part 3 and / or Part 5 of the Act.

²⁷ The terminology we have adopted in this report, and the groupings we have used for the purposes of our analysis, are not intended to correspond to the services in scope of the Government's announcement to restrict access by under 16s from certain social media sites.

- 2.29 This sample is not representative. Where we cite statistics or findings related to analysed services, they apply only to the services in the sample and should not be interpreted as indicative of sector-wide practices. Findings we cite from Ofcom research may reflect different services, methodologies and user experiences. Direct comparisons between our research and our findings in relation to analysed services should be made with caution.
- 2.30 For confidentiality reasons, we have redacted the names of service providers when discussing the information they provided in response to information notices. Where possible, we present the information provided by services in aggregated form.²⁸
- 2.31 We are engaging with analysed services to provide them with bespoke feedback on the information they provided about their approach to age assurance, including where they may have fallen short of our expectations. Where necessary, we may take further action as a result of the information provided.
- 2.32 These information notices were issued in December 2025, with data requested up until the end of November 2025. In some cases, service providers chose to provide data beyond this date, which we have included in relevant graphs and analysis where appropriate.
- 2.33 Some services have updated their approach to age assurance since we requested information. It should be noted that this report is based on the details contained in their information notice responses.
- 2.34 Alongside information notices, we also requested children’s access assessments from the sample of Part 3 pornography providers for details of their approach to age assurance.²⁹

Ofcom research sources on online experiences

- 2.35 We have used qualitative and quantitative research studies to understand how far children’s online experiences have changed since the age assurance duties came into force.
- 2.36 These sources include:
- **[Children’s Passive Online Measurement study \(CPOM\)](#)**: a passive measurement tracker of 8 to 14 year olds’ visits to websites and apps in a month across the smartphones, tablets and computers they use to go online. The study was conducted between October 2025 and March 2026.
 - **[Children’s Online Safety Tracker \(COST\)](#)**: a quantitative survey of UK children aged 8 to 17 recalled experiences of being online, including exposure to content that is harmful to them. Wave one was conducted March 2025 to April 2025 and wave two was conducted November 2025 to December 2025.
 - **[Proving Age to Access Online Pornography survey](#)**: a survey of UK internet users aged 16 and over who self-report having accessed pornographic content online,³⁰ to

²⁸ In redacting information and presenting it in aggregated form we have acted consistently with the requirements in section 393 of the Communications Act 2003 and section 164 of the Act.

²⁹ Part 5 services are not required to carry out children’s access assessments.

³⁰ This includes people aged 16 and over who have previously accessed pornographic content online – both those that have done so before and plan to again (“active users”) and those who have done so before but do not plan to again (“lapsed users”). As a result, data from this study is not based on a nationally representative sample. Instead, age and gender quotas were set to align with the demographic profile of X-rated adult site/app users, which resulted in more men in the sample (75% male versus 25% female).

understand how they access such content and their past experiences with age checks. Wave one was conducted in September 2025 and wave two was conducted in February 2026.

- **[Children’s experiences of being asked to verify their age tracker](#)**: a series of quantitative surveys looking at experiences of being asked to prove their age online among GB children aged 8 to 17 who have their own social media profile captured before and after the children’s safety duties came into force. Several waves of research conducted between July 2025 and January 2026.
- **[Parents’ Perceptions of Protection of Children Measures study](#)**: a quantitative survey of UK parents’ perceptions of protection of children measures including age assurance. Wave one of this study was conducted in July 2025 and wave two was conducted in October 2025.
- **[Adult Media Lives](#)**: an annual study with a panel of 20 people to track changes in media behaviour and explore how life experiences change people’s needs and shift their attitudes to digital media. The latest fieldwork was conducted in October 2025.
- **[Children’s use of virtual private networks \(VPNs\) study](#)**: a quantitative study looking at use of VPNs in the 6 months prior to fieldwork among GB children aged 11 to 17. Fieldwork conducted in March 2026.
- **[Children and Parents: Annual Media Use and Attitudes Report \(CaP\)](#)**: a longitudinal study that provides evidence on media access, use, attitudes and understanding among children aged 6 months to 17 years old. The latest fieldwork was conducted between November 2025 and February 2026.
- **Ipsos iris audience measurement service**: a passive single-source representative panel of over 10,000 UK people aged 15 and over who use the internet. A passive tracker measures the panellists’ use of websites and apps across the smartphones, tablets, and computers that they use to go online.
- **Similarweb**: a digital intelligence platform that estimates and analyses online behaviour, traffic, audiences, and market trends across websites, apps, search engines, ecommerce services, and AI platforms. All data made available by Similarweb is estimated based upon data obtained from third parties and is intended for informational purposes only. Ofcom analysis is based on approximately 21,000 adult services operating in the UK, and aggregated usage data for VPN mobile apps across Android and iOS devices.

2.37 We have included findings which reference specific services from these studies only where they are already in the public domain and they are relevant for the purpose of this report.

2.38 Where necessary these sources have been supplemented with Ofcom’s own analysis, for example regarding the presence of age assurance on pornography services.

2.39 We expand on these research sources and recognise limitations to the report in Annex A1.

Report structure

2.40 This report is structured as follows.

- **Section 3** provides an overview of age check deployment and adoption across industry.
- **Section 4** sets out a sector-level assessment of pornography services.

- **Section 5** sets out a sector-level assessment of social media services.
- **Section 6** sets out a sector-level assessment of dating services.
- **Section 7** provides a cross-cutting assessment of factors that have prevented or hindered the effective use of age assurance.
- **Section 8** sets out a summary of issues and suggested improvement based on evidence in this report.
- **Annex 1** sets out our detailed methodology, including research sources and limitations.
- **Annex 2** provides detailed analysis of how services had regard for the criteria and principles in our HEAA guidance.
- **Annex 3** provides further analysis on cost and choice of age assurance methods.
- **Annex 4** sets out a glossary of terms used in the report.

3. Age assurance use and effectiveness across industry

Key findings

- **The volume of completed age checks has significantly increased across all sectors since July 2025.** Between July and December 2025, over 69 million age checks were completed across analysed services in the UK— a 23-fold increase on the previous six months.
- **Highly effective age assurance methods have been widely deployed across industry.** All analysed services offered at least one method included in our HEAA guidance, with facial age estimation and photo ID matching the most commonly deployed.
- **Analysed services demonstrated regard for our highly effective age assurance criteria when implementing their age assurance processes,** but there is room for improvement, and we have set out steps to this effect.
- **Age assurance is increasingly shaping children’s online experiences,** but there is more work to be done to increase the impact of age checks on children’s safety online. This includes where age checks have not been deployed at all, and where they are in place but not effective enough.

Use of age assurance across industry

The volume of completed age checks has significantly increased across all sectors since July 2025

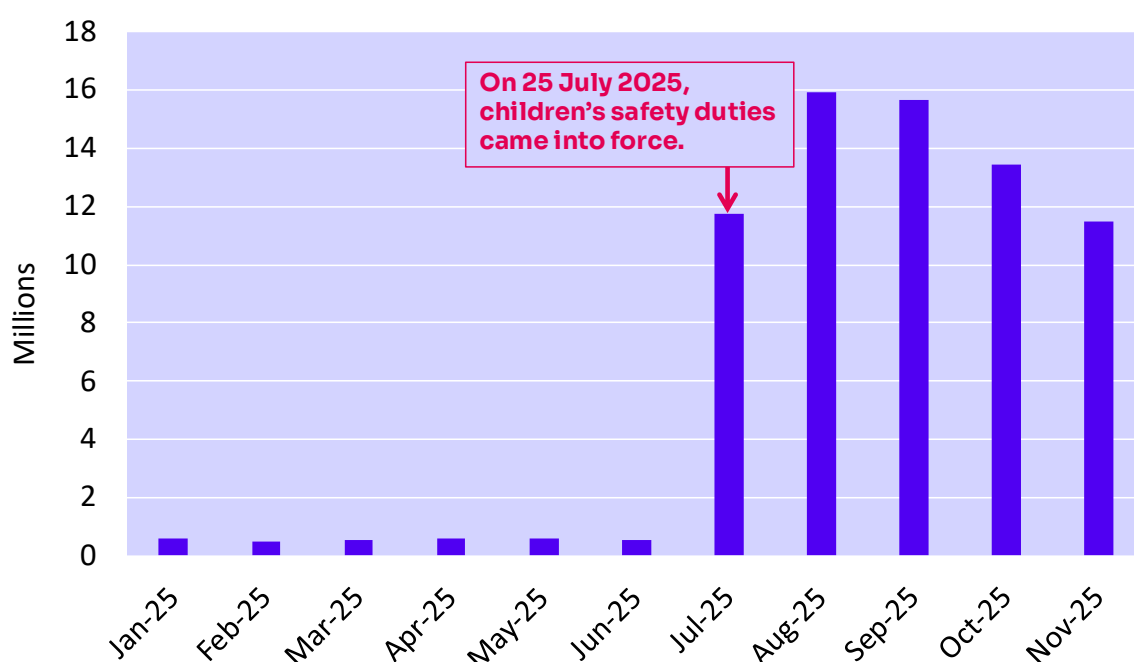
- 3.1 Since the children’s safety duties came into force in July 2025, there has been widespread adoption and use of age assurance across services in the pornography, social media, dating, and gaming sectors.
- 3.2 Based on data collected via information notices, over 69 million age checks were completed between July and December 2025 across the 32 services analysed in this report (shown in Figure 1).³¹ This represents a 23-fold increase on the 3 million checks completed by these services in the previous six-month period.³²

³¹ The true figure is likely higher due to data from July and December 2025 being incomplete. For most analysed services, age assurance was implemented on or around 25 July 2025 meaning that data for July 2025 is from a shorter period. Only some services provided data for the month of December 2025.

³² These figures represent only analysed services and therefore will underrepresent the total number of age checks taking place across all services with age assurance in place. They also exclude the number of checks carried out via age inference models on the basis that these models generate an estimate for each user (usually on a frequent basis) and would skew the data if included alongside the number of active age checks that analysed services have conducted.

- 3.3 Figure 1 shows that the total number of completed age checks peaked in August 2025 and gradually declined afterwards. This likely indicates that many of the analysed services retained the result of a user's initial age check (whether by associating it with an account or device or otherwise binding the result of the age check to a user), rather than requiring individual users to repeat age checks each time they used a service.
- 3.4 Our research into children's online experiences reflects this large-scale deployment. Exposure to age assurance methods (excluding self-declaration) rose from 25% in July 2025 to 43% in January 2026.³³ Among 8 to 17-year-olds who recalled being asked to prove their age, facial age estimation was the most commonly recalled method.³⁴

Figure 1: Total number of age checks completed across analysed services from January to November 2025.



Source: Data from analysed services' responses to information notices

- 3.5 In response to our 2025 Call for Evidence: Statutory reports on age assurance and app stores (our 2025 CfE), several stakeholders described the high level of age assurance implementation since the children's safety duties came into force,³⁵ with the Age Verification Providers Association (AVPA) stating that the rollout of age assurance

³³ Ofcom, 2026. Children's experiences of being asked to verify their age tracker. When we refer to 8 to 17-year-olds in these findings, we mean GB children aged 8 to 17 who had their own profile on at least one of the social media sites or apps about which we asked and these specific data are based on the sub-set of this group who said they had ever been asked to prove their age. See methodology annex for further details of methodology. Fieldwork in July 2025 took place before duties came into force.

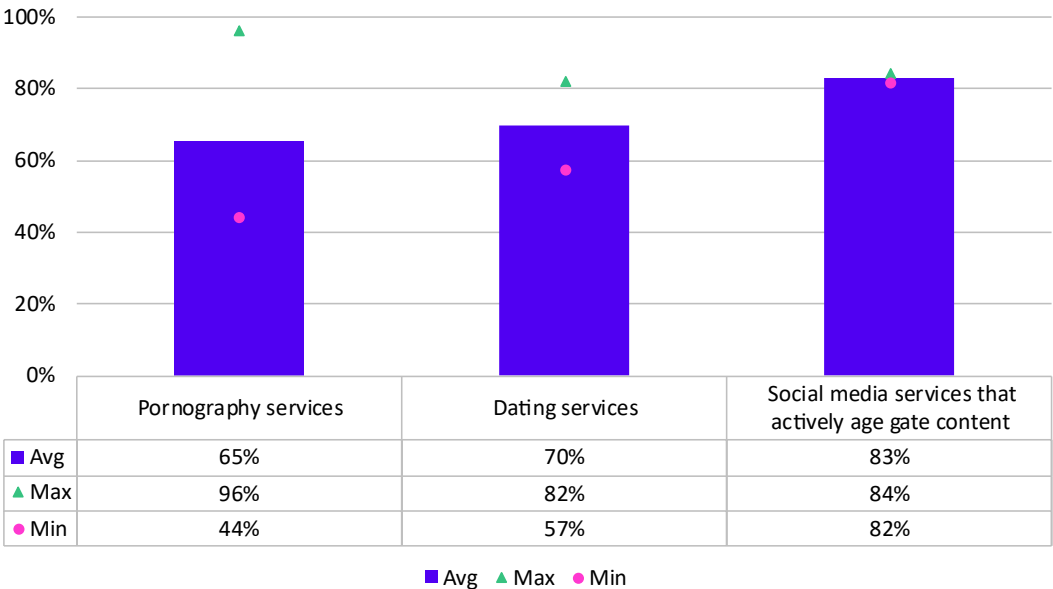
³⁴ Ofcom, 2026. Children's experiences of being asked to verify their age tracker.

³⁵ Online Dating and Discovery Association (ODDA) response to our 2025 CfE, p.2; [§<] response to our 2025 CfE, p.2; VerifyMy response to our 2025 CfE, p.1.

represented the largest coordinated deployment of age checks ever seen at a national scale.³⁶

3.6 The average percentage of users determined as over 18 (or above the respective challenge age) out of those who completed an age check across all analysed services between July 2025 and November 2025 was 57.8%. However, the percentage of users³⁷ determined to be aged 18 or over varied significantly across service types, as shown in Figure 2.^{38 39} This could reflect the efficacy of services’ approach to age assurance in places, but also likely reflects a number of other factors, including the underlying population of users that are undergoing the age checks on each service and the specific context of the age check (i.e. whether it is deployed at the point of entry to the service, to age-gate specific content, or at specific trigger points).

Figure 2: Average proportion of users that completed an age check who were determined to be 18 or over for each service type from July 2025 to November 2025. The data markers indicate the highest and lowest service percentages within each service type.



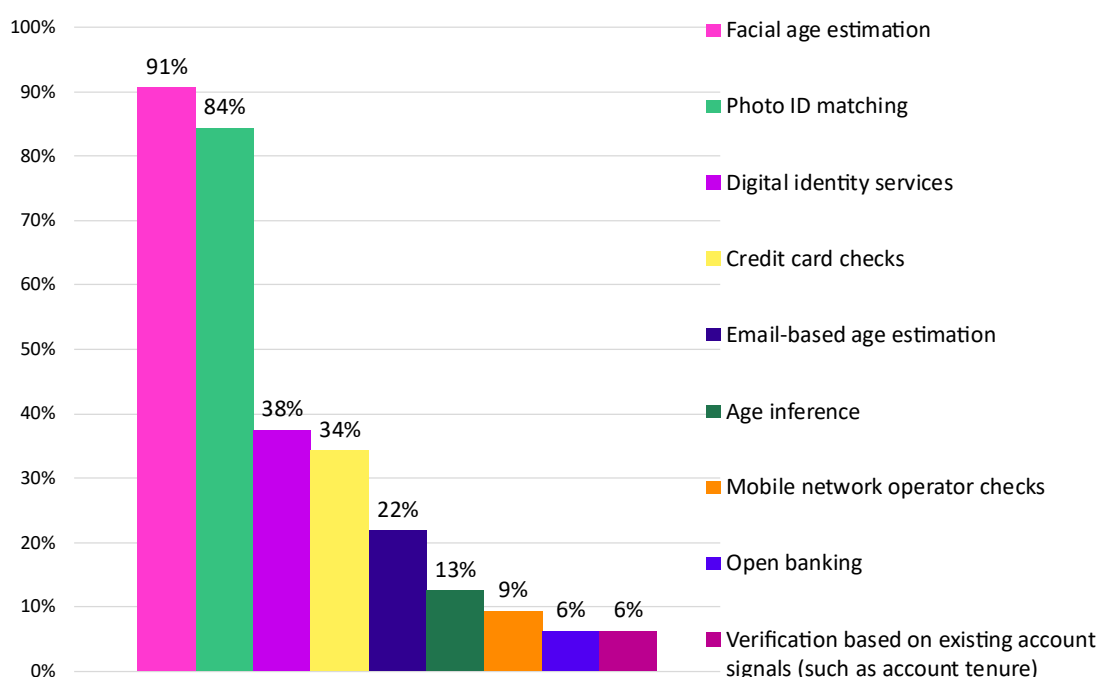
Source: data collected via information notices to analysed services.

³⁶ Age Verification Providers Association (AVPA) response to our 2025 CfE, p.2.
³⁷ In our information notices we requested information about ‘active UK users’ as defined in the Glossary in Annex 5. In the case of pornography services, a ‘user’ includes those who may visit the service but not gain access if the age check does not determine them to be 18 or over.
³⁸ We cannot determine from information notice data what proportion of these users would then go on to pass a subsequent age check to gain access to the site or content.
³⁹ We have not included social media services who use passive age inference in this analysis, because the outcomes of their approach to age assurance are explored in Section 5.

Highly effective age assurance methods have been widely deployed across industry

3.7 In our HEAA guidance, we included seven methods we consider capable of being highly effective; all analysed services offered at least one of these methods.⁴⁰ Some methods were offered more frequently than others. Facial age estimation was the most offered method, followed by photo identification (photo ID) matching (as shown in Figure 3). Most analysed services offered multiple methods, with three being the average number of age assurance methods deployed.

Figure 3: Percentage of analysed services who deployed each type of age assurance method.



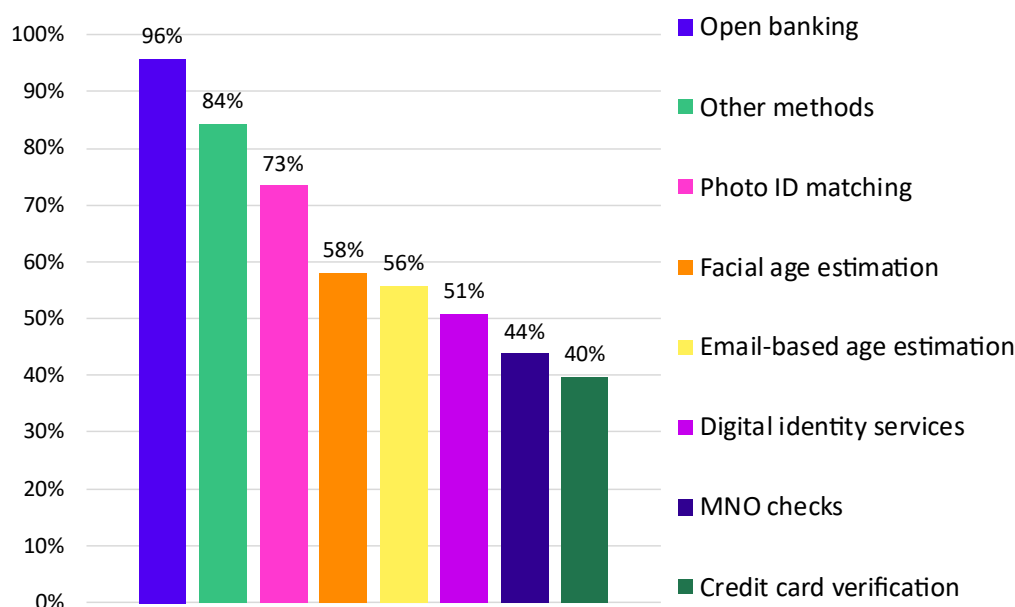
Source: Data from analysed services' responses to our information notice issued 15 December 2025.

3.8 The effectiveness of different age assurance methods was a common theme in response to our 2025 CfE.⁴¹ While not a direct indicator of effectiveness, evidence gathered via information notice (shown in Figure 4) indicates that the proportion of users determined to be aged 18 or over varied significantly by method. This is likely driven by a number of factors in addition to any differences in technical capability, including: accessibility of the method including whether the user needs specific proof of identity or hard identifiers; user behaviour and perceptions of different methods; and ease of use and time required to complete an age check.

⁴⁰ Part 3 HEAA guidance and Part 5 HEAA guidance. The methods we listed are: (1) open banking; (2) photo identification (photo ID) matching; (3) facial age estimation; (4) Mobile network operator (MNO) age checks; (5) credit card checks; (6) email-based age estimation; and (7) digital identity services.

⁴¹ [3<] response to our 2025 CfE, pp.4-5; [3<] response to our 2025 CfE, p.5; [3<] response to our 2025 CfE, pp.2-3; [3<] response to our 2025 CfE, p.2.

Figure 4: Percentage of users determined as 18 or over, split by method



Source: Data from analysed services' responses to our information notices issued 15 December 2025

3.9 Further detail on method deployment is outlined in the sector specific sections of this report.

Analysed services demonstrated regard for our highly effective age assurance criteria when implementing their age assurance processes, but there is room for improvement

- 3.10 Overall, analysed services demonstrated that they had regard to the criteria and principles set out in our HEAA guidance, though the extent of this varied and there remains scope for some services to improve.
- 3.11 Most services considered technical accuracy when selecting and deploying age assurance methods, often referencing performance metrics such as precision, recall and false positive rates, with many services relying on third-party testing or certification schemes.
- 3.12 On the demonstration of robustness, some services described testing across devices and conditions. Most analysed services had taken steps to mitigate circumvention, including the use of liveness detection alongside facial age estimation and/or photo ID matching.
- 3.13 For the criteria of reliability, services commonly relied on independent testing, certification, and provider assurances, and some reported conducting internal quality assurance activities including reviews of model performance, testing changes prior to deployment and internal monitoring of age assurance outcomes.
- 3.14 Services showed regard for fairness through demographic testing and, in some cases, model retraining where disparities were identified.

- 3.15 Services demonstrated that they had considered the principle of accessibility through offering multiple methods and user support features and recognised the importance of ensuring that age assurance is easy to use and works for all users.
- 3.16 In general, services were not yet using interoperable age assurance solutions. However, some services stated that they were monitoring developments or beginning to invest in this area.
- 3.17 We also asked services about their appeals processes. While some analysed services stated that they had an appeal process involving some form of customer support or manual reviews,⁴² other services offered users the option to attempt one or more alternative age assurance methods.⁴³ In some cases users can only retry the same method.⁴⁴ Only six services provided us with data on the number of appeals that were upheld.⁴⁵ Overall, the lack of data that analysed services provided us with on appeals and appeals upheld, coupled with the fact that many services do not offer users an appeal process at all, reinforces the need for services to implement appeal processes and monitor their appeal numbers.
- 3.18 In Annex 2, we provide a more detailed analysis of services' regard for our HEAA guidance. Based on this analysis, we set out areas for improvement in Section 8. We expect all service providers that are required to implement age assurance to consult these.

Effectiveness of age assurance across industry

- 3.19 The evidence base for this report is largely drawn from the first six months after the children's safety duties came into force. For this reason, this report is not intended to offer a definitive conclusion on whether age assurance is effective for the purpose of complying with duties under the Act. No single evidence source provides a conclusive answer on effectiveness, and together they present a nuanced picture of the impact of age assurance so far.

Age assurance is increasingly shaping children's online experiences, but some services are still failing to deploy highly effective age checks

- 3.20 Evidence suggests that age assurance is having a meaningful impact on children's experience online. Firstly, children increasingly report seeing age checks online: in January 2026 43% of 8-17s who recalled an age check encountered highly effective age assurance methods, an increase from 25% in July 2025.⁴⁶ Secondly, our passive measurement study found that some children are still attempting to access pornography, but in many cases the

⁴² [X] 15 analysed services' responses to our information notices issued 15 December 2025.

⁴³ [X] 15 analysed services' responses to our information notices issued 15 December 2025.

⁴⁴ [X] 2 analysed services' responses to our information notices issued 15 December 2025.

⁴⁵ [X] 6 analysed services' responses to our information notices issued 15 December 2025.

⁴⁶ Ofcom, 2026. Children's experiences of being asked to verify their age tracker. When we refer to 8 to 17-year-olds in these findings, we mean GB children aged 8 to 17 who had their own profile on at least one of the social media sites or apps about which we asked and these specific data are based on the sub-set of this group who said they had ever been asked to prove their age. See methodology annex for further details of methodology. Fieldwork in July 2025 took place before duties came into force.

presence of age assurance appears to deter them.⁴⁷ Finally, a relatively small proportion of children reported to us that they have used a VPN to access content or features intended for people older than them (although it must be noted that this may understate the proportion of children circumventing these restrictions due to response bias).⁴⁸

3.21 However, there is more that services can do. In Section 4: Pornography services, Section 5: Social media services, and Section 6: Dating services, we assess the effectiveness of age assurance by sector. In summary, we observed the following for each sector:

- a) In the **pornography industry**, evidence indicates that age assurance is deterring children and reducing their access to some of these services. However, the overall effectiveness of age assurance in the pornography sector has so far been constrained by the large number of pornography services that have not implemented age assurance. Some children are still visiting pornography services and about half of those we studied were able to access one without age assurance. In many cases this is facilitated by search engines. This suggests that age assurance is proving effective at the individual service level when deployed correctly and in line with our HEAA guidance, but not yet at an overall system level, due to user migration to non-age assured sites.
- b) Many **social media services** have taken steps to implement age assurance, but our research indicates the proportion of children encountering any harmful content online remains unchanged. And, while we have seen some reduction in exposure to the most harmful kinds of content for some services, other kinds have been reported by more children since the children's safety duties came into force. Additionally, our evidence suggests variability in the capability of age inference models (which some services have chosen to use), and in some instances we are concerned that some service providers have not effectively detected the children on their services.
- c) Evidence suggests that in December around one in ten 15 to 17-year-olds were spending time on **dating services** that had age assurance in place to prevent child access.⁴⁹ This suggests that, as of December 2025, the presence of age checks seems to have had little impact on older teens' use of these sites/apps. However, following engagement with Ofcom, dating services are taking steps to address identified issues and improve the effectiveness of their age assurance process, such as implementing challenge ages and liveness detection.

3.22 Throughout the report we set out issues and areas where services should improve their age assurance process, based on our observations of where services' age assurance implementation has fallen short of our expectations. Our observed issues and suggested improvement are outlined in full in Section 8. In summary, the three main areas for improvement are:

- Follow our HEAA guidance in full; and

⁴⁷ Ofcom, 2026. Children's Passive Online Measurement – Pornography Services Report. 7% of 8 to 14-year-olds visited at least one pornography service with age assurance, with 4% of 8 to 14 year olds only visiting pornography services with age assurance.

⁴⁸ Ofcom, 2026. Children's Use of VPNs. Five per cent of children in this study said they had used a VPN in the past six months to either access content meant for people older than them, or to access features and functions with age restrictions.

⁴⁹ Ipsos, Ipsos iris UK online measurement service, app only – December 2025 among UK internet users aged 15-17. These findings are detailed in section 6.

- Conduct regular due diligence on any age assurance vendors you employ, and your age assurance process; and
- Comply with your privacy and data protection obligations.

3.23 Services should consult our HEAA guidance, review their existing age assurance process against our areas for improvement and implement the necessary changes. See Section 8 for the full list of practical improvements that services should take. We will continue to take action to secure compliance with the protection of children duties, including enforcing against services that are not complying with their duties to protect children.

4. Pornography services

Key findings

- **Age checks have been deployed at scale in the pornography industry.** The top 10 most popular pornography services in the UK have all implemented age assurance. 64 out of the top 100 most popular pornography services in the UK have deployed age assurance as of June 2026, with a further 10 geo-blocking UK users.
- **All analysed pornography services implemented age assurance using methods included in our HEAA guidance.** Services generally offered multiple methods, used a challenge age approach, and deployed liveness detection.
- **Highly effective age assurance is helping to prevent children from accessing pornography online.** Evidence shows that a small proportion of children in the UK continue to seek out pornographic content, but half of these children only visited services with age assurance and spent little time there.
- **However, it is still too easy for children to find pornography services without age checks in place.** Our research shows that almost half (47%) of the pornography services visited by children have no age checks in place.
- **In some cases, children find these sites via search engines.** Our analysis shows that pornography services without age assurance frequently appear in search queries.
- **This means that more action is needed as part of a system-wide effort.** Given the scale and nature of the online pornography sector, there are questions about the role that other actors in the ecosystem can, and should, play, including search engines, operating systems, and app stores, to increase effectiveness and strengthen protections for children.

Age assurance implementation: scale and approach

The majority of the top 100 pornography services in the UK have implemented age assurance

- 4.1 As of June 2026, 64 of the top 100⁵⁰ most popular pornography services in the UK had deployed age checks, up from 41 services in August 2025, the month after the children's safety duties came into force. This includes all of the top 10 most popular pornography services, which account for around one fifth of all UK visitors to adult sites.⁵¹ The 36

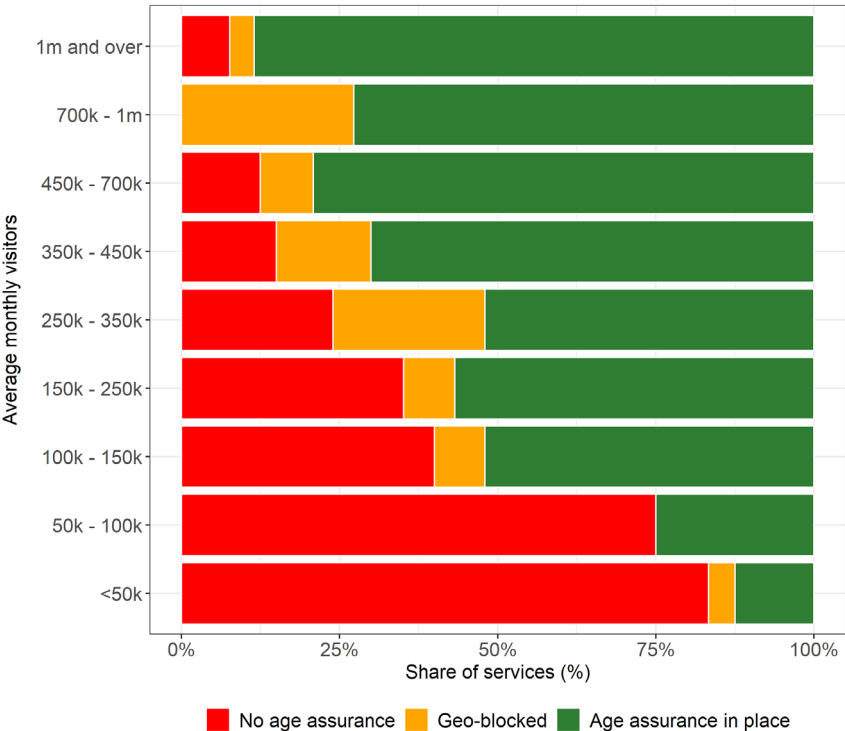
⁵⁰ The top 100 is roughly 0.5% of the adult sites likely to be in scope of the Act, but it accounts for over 20% of all UK visitors to adult sites.

⁵¹ Analysis conducted using a combination of Similarweb data and manual checking by Ofcom. The dataset of 21,000 adult websites from Similarweb includes pornographic sites and other adult site types: non-pornographic sites such as Ann Summers; adult service websites; and others have been removed in our

pornography services without age assurance included ten services that restricted access from the UK (such as geo-blocking), with the remainder still displaying pornographic content without age checks.

- 4.2 Evidence suggests that age assurance deployment may be strongly related to traffic levels. Using data from Similarweb,⁵² we grouped the top 200 most popular pornography services by their estimated monthly UK traffic prior to the children’s safety duties coming into force.⁵³ As shown in Figure 5, lower-traffic services are considerably less likely to have age checks in place: 25% or fewer of these services have implemented age assurance, compared with around 90% among higher-traffic services.

Figure 5: Estimated monthly traffic and age assurance deployment



Source: Similarweb. 226 pornography services analysed using estimated monthly traffic from April 2025 to June 2025. Data extracted on 03 June 2026. Age assurance deployment as of April 2026.

- 4.3 Different factors may explain this pattern, for example financial constraints may limit the capacity of services with less user traffic to implement and maintain age assurance. As further discussed in Section 7, age assurance is associated with direct costs that some

internal analysis of the top 100 and top 200 but not for analysis relating to a wider set of sites. As a result, we use two different terms: “adult sites” for the wider set of sites and “dedicated pornography services” or “pornography services” to refer to the smaller, vetted list.

⁵² Similarweb defines monthly visitors as the average number of individuals visiting the analysed website in a given month. All data made available by Similarweb is estimated based upon data obtained from third parties and is intended for informational purposes only.

⁵³ We used average monthly estimated visitors before the rollout of age assurance (April 2025 to June 2025) to group services into traffic categories. This is because traffic can vary significantly conditional on age assurance deployment, decreasing for services with age checks in place and increasing for those without. As such, using estimated monthly visitors after July 2025 could mask the underlying relationship between traffic and deployment.

businesses may struggle to absorb, as well as significant indirect costs, such as reduced user traffic and associated revenue effects which may further discourage adoption.

Where an age gate is placed in the user journey varies, but analysed services have most frequently taken the safest approach

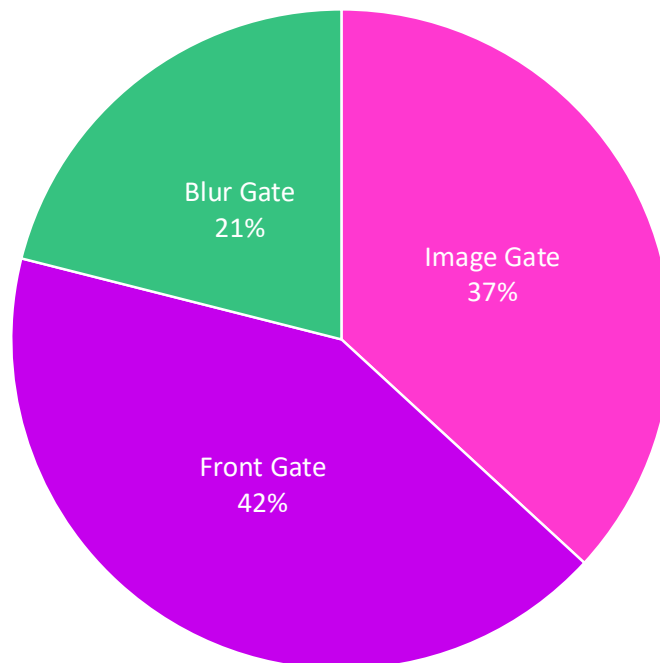
- 4.4 Under the Act, pornography services are required to restrict access at the point of entry to the service, but they can do this in a variety of ways.
- 4.5 In January 2026, we set out four types of age gate being used across dedicated pornography sites in the UK:⁵⁴
- a) **Front gate:** A user sees only a blank landing page, with no content visible until they have completed the age check.
 - b) **Blur gate:** A user sees a series of blurred images before the age check. In some cases, titles are visible which could contain strong sexual wording. Clicking on a thumbnail directs users to an age check.
 - c) **Image gate:** A user sees a series of clearly visible images. Often these are of clothed people, sometimes in sexually suggestive poses and/or wearing underwear. In some cases, titles are visible which could contain strong sexual wording. In some variations, users can see a preview of the video when hovering over with a cursor. Clicking on the thumbnail directs users to an age check.
 - d) **In-video gate:** A user sees a series of thumbnails that contain clearly visible images. Often these are of clothed people, sometimes in sexually suggestive poses and/or wearing lingerie. In some cases, titles are visible which could contain strong sexual wording. Users can sometimes see a preview of the video when hovering over with a cursor. Users can then watch the video up until a certain point, usually up until nudity is shown, after which they are directed to an age check.
- 4.6 Our Protection of Children Code recommends services restrict access to the entire service and all content, pornographic or otherwise, until an age check has been completed and the user has been determined to be over 18 (the front gate approach). The front gate is the safest placement for an age gate on a pornography service.
- 4.7 The alternative approaches that some services have taken allow the user to access some form of non-pornographic content prior to completing an age check (such as an image gate, blur gate, or in-video gate). These approaches carry significantly more risk of children encountering pornographic content on the service, because their effectiveness depends on services ensuring that the content accessible to all users prior to the age check does not meet the definition of pornographic content.⁵⁵ In practice, this requires the accurate identification of pornographic content before it is made available without an age check.
- 4.8 Figure 6 shows the distribution of age-gate approaches across analysed services as of early April 2026. The front gate was the most common approach used, followed closely by services using an image gate. No services used the in-video gate. This may be due to the

⁵⁴ Ofcom, 2026. [Age checks: Why their placement matters in pornography](#).

⁵⁵ Pornographic content is defined in the Act as “content of such a nature that it is reasonable to assume that it was produced solely or principally for the purpose of sexual arousal”; see further our [Guidance on content harmful to children](#), p.14.

publication of [our blog](#) outlining the concerns we had with this approach. Of the total of 118 different pornography services with age assurance that were visited by panellists in our Children’s Passive Online Measurement study, 45% had a front gate, 39% had a blur gate, 14% had an image gate and 2% had an in-video gate.

Figure 6: Distribution of analysed pornography services using types of age gate.



Source: Internal Ofcom information-gathering.

4.9 In the following subsection we look in more detail at how the effectiveness of age assurance on pornography services affects children’s online experiences.

Analysed pornography services have deployed age assurance methods that we recommended in our HEAA guidance

4.10 Analysed pornography services have almost exclusively relied on age assurance methods included in the non-exhaustive list of our HEAA guidance as capable of being highly effective. The only exception to this was a form of age check based on the length of time a user had their account, which was used alongside other methods of age assurance capable of being highly effective.

4.11 Data collected from analysed services indicated that 16 of the 19 analysed pornography services had deployed facial age estimation and/or photo ID matching, making these the most common methods offered. All but two pornography services using facial age estimation applied a challenge age approach, as recommended in our HEAA guidance.⁵⁶ The

⁵⁶ A challenge age approach is widely used offline when selling age-restricted products in retail environments, for instance, through the retailing strategy ‘Challenge 25’. In an online age assurance process, a challenge age approach refers to where a user who is estimated as being under a given challenge age must then undergo a second age assurance step (for example, a different age assurance method) to confirm that they are over the required age. For more details, see paragraphs 4.16-4.20 of our Part 3 HEAA guidance.

remaining two services had multiple age assurance providers for their facial age estimation solutions, of which one did not use a challenge age. One of these services described their particular facial age estimation solution as being a “no threshold model”⁵⁷ while the other said that their solution “does not have any predefined challenge age thresholds” and instead applies “a multi-layer AI model to determine age”.⁵⁸ Implementing a challenge age is key to the overall effectiveness of the age assurance process. It is the services’ responsibility to ensure that the solution they use is configured appropriately so that risks around the age boundary are systematically mitigated. Where it is not technically feasible to apply a challenge age, then we would expect services to demonstrate an alternative mechanism that is equally as effective as a challenge age at reducing the likelihood of false positives.

- 4.12 All 12 of the analysed services that used digital identity services as an age assurance method were pornography services. Some digital identity services provide reusable age checks, allowing a verified result to be used across multiple services that use the same digital identity services provider, thereby reducing the need for repeated age checks. However, information notice data on age check completions indicated that only 2% of completed age checks on analysed pornography services used digital identity services, showing a slower uptake compared with other methods. One pornography service provider removed digital identity services after a week of using it because its experience was that the user flow was “long”, and it saw evidence of users abandoning the process.⁵⁹
- 4.13 According to data from analysed services, facial age estimation was by far the most common method among users completing an age check, making up 68% of all age check completions between July and November 2025 for analysed pornography services. Evidence from the Proving Age to Access Pornography Online survey similarly shows that a majority of active users of pornography online⁶⁰ who reported ever completing an age check said they had used facial age estimation (58%) for this purpose, with photo ID matching (28%) the next most common method.⁶¹
- 4.14 Data from analysed services showed that email-based age estimation and mobile network operator checks were also popular methods among users completing an age check. Each method accounted for 12% of all age check completions across analysed pornography services, despite only being offered by five and two services, respectively. One pornography service provider did not offer facial age estimation and instead gave users a choice between five other methods.⁶² We have used this as an illustrative example of how users have selected an age assurance method when given this choice. Of these five methods, email-based age estimation was the most used by far, making up 55% of the age checks completed between July and November 2025, followed by mobile network operator checks at 24%. See Figure 7 for more details.

⁵⁷ [X] response to our information notice issued 15 December 2025.

⁵⁸ [X] response to our information notice issued 15 December 2025.

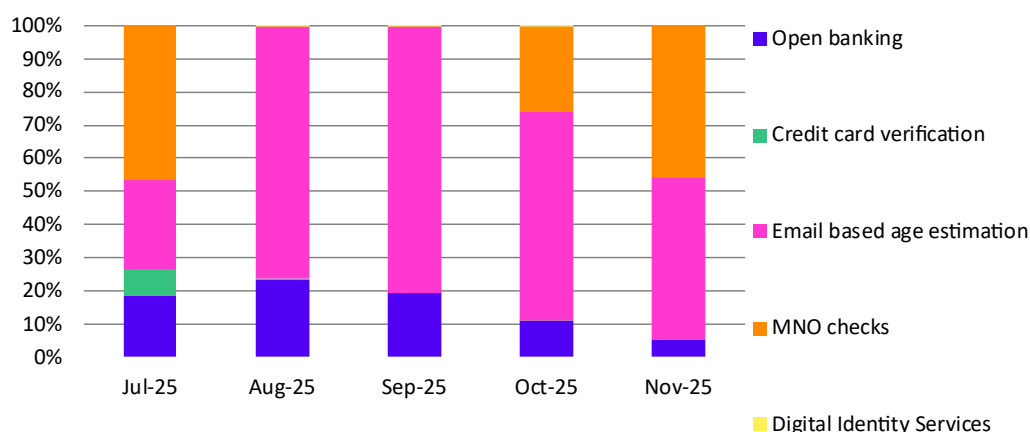
⁵⁹ [X] 3 analysed services’ responses to our information notices issued 15 December 2025.

⁶⁰ By “active users of pornography online” we mean people aged 16 and over who have previously accessed pornographic content online and plan to do so again.

⁶¹ Ofcom, 2026. Proving age to access pornography online.

⁶² [X] 2 analysed services’ responses to our information notices issued 15 December 2025.

Figure 7: Percentage of users who opted to undergo each age assurance method on one analysed pornography service provider from July to November 2025



Source: Data from analysed services' responses to our information notice issued 15 December 2025.

- 4.15 Our Proving Age to Access Online Pornography Survey suggests greater comfort with age estimation methods (facial and email-based) than with age verification methods. Among active and lapsed users of pornographic content online, eight in ten indicated that they felt uncomfortable using credit card checks to prove their age in order to access pornography online. This combined group of active and lapsed users included a small proportion (6%) of users of paid-for pornography services.⁶³ On paid-for pornography services where a user has already provided credit card details to access the service, credit card checks offer a low-friction method that is capable of being highly effective.
- 4.16 In our HEAA guidance, we said that services can improve accessibility by offering users more than one age assurance method to choose from. We have seen that many of the analysed pornography services do this. All analysed pornography services offered users more than one method to prove they are an adult, with the average being three methods.⁶⁴ Three of the pornography services reported using a wider range of methods within our HEAA guidance initially before narrowing down to a smaller subset over time, guided by what worked for their users.⁶⁵
- 4.17 Almost all analysed pornography services relied exclusively on third-party vendors, with only one analysed pornography service using an in-house solution.⁶⁶ Some service providers cited privacy considerations as influencing their choice of a third-party provider, including comments around the processing and retention of age assurance data and that they receive minimal outcome signals from third-party age assurance providers.⁶⁷

⁶³ Ofcom, 2026. Proving Age to Access Online Pornography Survey.

⁶⁴ This is the mean number of methods offered, rounded to a whole number.

⁶⁵ [3] 3 analysed services' responses to our information notices issued 15 December 2025.

⁶⁶ [3] response to our information notice issued 15 December 2025.

⁶⁷ [5] 5 analysed services' responses to our information notices issued 15 December 2025. More detailed discussion of user privacy and data protection can be found in Section 7.

Effectiveness of age assurance for pornography services

- 4.18 For the use of age assurance to be effective on dedicated pornography services, it must prevent children from accessing pornographic content. If this is the case in practice, we would expect to see children spending less time on dedicated pornography services and encountering pornographic content via these services less often.
- 4.19 The evidence available to us at this early stage suggests that, where implemented in line with our HEAA guidance, age assurance seems to be reducing access to dedicated pornography services. However, this effect has been limited by children turning to services without age checks to seek pornographic content.⁶⁸
- 4.20 The following section relies predominantly on our CPOM Study. The aim of CPOM is to directly observe and measure the internet use of UK children aged 8 to 14. For more information about the study, specific findings, and its methodology, see the [CPOM report](#) on pornography services.

Eight per cent of online 8 to 14-year-olds visited a pornography service in a month

- 4.21 Our CPOM study conducted between October 2025 and March 2026 found that 8% of the panel of online UK 8 to 14-year-olds visited a pornography service in a month,⁶⁹ with most children spending little time on individual sites. Half of these children only visited a site with age assurance.
- 4.22 In this study, a “visit” refers to a website or app that has been opened on the passively tracked device for a duration of 1 second or longer.⁷⁰ Importantly a “visit” does not necessarily mean that the person viewed pornography. For example, it includes visits where the only page seen was a notice to complete an age check, or a message saying the site was not available in the UK because of geo-blocking. Similarly, the passive tracking technology used in this study does not record whether someone actually viewed pornographic content. Instead, we use measure such as how often sites are visited, the length of the visits, how people navigate within a session and patterns of use across services to estimate the likelihood that pornographic content was viewed.⁷¹
- 4.23 In total the 8% of children in the CPOM panel visited 257 different services during the study, on average visiting five different pornography services across a month. A small number of children took part in, and visited pornography services in, both phases of our study. Among these five children, four visited more services in the second phase. Analysis of their

⁶⁸ Ofcom, July 2026. [Children’s Passive Online Measurement \(CPOM\) – Pornography Services Report](#).

⁶⁹ In this study, one month is 28 days.

⁷⁰ Visits of less than one second are not counted to limit the impact of advertising pop ups and other automated redirects in the final data.

⁷¹ It should also be noted that checks as to whether services had age assurance and the placement of the age gates took place in the analytical phase of our study. At the time of fieldwork, the presence and placement of age gates on some services may have been different. Where it was known that the age gate type was different during the CPOM fieldwork period, that age gate type has been applied to the analysis.

journeys indicate they may have been looking for a site where they were able to access pornography.⁷²

- 4.24 We also observed that while 8% of children visited pornography services, some spent such a short amount of time on them that it suggests they may not have accessed pornography on most, or potentially all, their visits. Almost two-thirds (65%) of all pornography service visits lasted less than 10 seconds, and a further 22% lasted between 10 and 30 seconds. Taken together, nearly nine in ten (87%) pornography service visits were for under 30 seconds. The number of visits combined with very low visit duration on individual service visits suggests many panellists were moving quickly between sites, via short, transient visits – potentially in search of a site they could access without an age check.⁷³

Half of children that visited pornography services only visited sites with age assurance

- 4.25 Our study found, 7% of 8 to 14-year-olds visited at least one pornography service with age assurance, with 4% of 8 to 14-year-olds only visiting pornography services with age assurance. Of the total of 257 different pornography services visited by panellists during the study, 118 (46%) had age assurance deployed.^{74 75}
- 4.26 Some children on the CPOM panel participated in the two studies, before and after the implementation of age assurance. As noted above, five of these children visited pornography services in both studies, which allows us to see how their visits to services which have implemented age assurance have changed. Among this small subset of children, visits to Pornhub, which implemented age assurance in July 2025, fell sharply from 122 visits in the first phase, to eight visits in the second. Only one child in the second phase visited the service more than once. This indicates that children may have attempted to access Pornhub but did not repeatedly visit the service, demonstrating that age assurance may be effective at deterring children from accessing pornography services.⁷⁶
- 4.27 Children experienced the range of age gates and evidence suggests that the front gate approach appears the most effective. Children spent less time on these services with a front gate approach and spent significantly longer on services with image gates, indicating that children may have spent time browsing the service anticipating that they had access to the service before then encountering age assurance. While this does not necessarily mean that age restrictions have been bypassed, it highlights the increased risk of these approaches, as the service must ensure these images are entirely free of pornographic content.⁷⁷

⁷² Ofcom, July 2026. Children's Passive Online Measurement (CPOM) – Pornography Services Report.

⁷³ Ofcom, July 2026. Children's Passive Online Measurement (CPOM) – Pornography Services Report.

⁷⁴ The age assurance status of these services was checked after fieldwork was conducted and for most services is correct as of May 2026. Where it was known that the age gate type was different during the CPOM fieldwork period, that age gate type has been applied to the analysis. See main report for further detail.

⁷⁵ Ofcom, July 2026. Children's Passive Online Measurement (CPOM) – Pornography Services Report.

⁷⁶ Ofcom, July 2026. Children's Passive Online Measurement (CPOM) – Pornography Services Report. From 2 February 2026, Pornhub introduced further restrictions by preventing new user registrations in the UK. At the same time Pornhub added non-pornographic content to its landing page.

⁷⁷ See our Guidance on content harmful to children, p.14 for more information on how pornographic content is defined.

However, some children purposefully sought out pornographic content and used search services to find services without age assurance

- 4.28 While it seems that age assurance creates friction and prevents access when implemented as a highly effective process, in some cases children sought out pornography through services without age assurance. Four per cent of children in the CPOM panel visited 121 different services that had accessible pornographic content and therefore most likely encountered pornographic content.⁷⁸
- 4.29 Individual user journeys paint a picture of user migration from services with age assurance to those without. One 14-year-old boy only visited Pornhub in the first phase of research and went on to visit 25 different pornography services in the second phase.⁷⁹
- 4.30 Search services play a role in the discovery of pornography services without age assurance. Many (62%) children who visited pornographic services in our study used a search engine immediately before visiting pornography services, at least once.⁸⁰ This demonstrates an intent to view pornography as opposed to a child accidentally stumbling upon it.⁸¹
- 4.31 One 14-year-old boy in the study entered explicit search terms into search services as well as circumvention-related search queries. During one session this boy visited 15 different pornography services, some of which had age assurance in place and some of which did not. The boy switches between Google search and pornography services for 25 minutes, moving from one to the next rapidly, often spending less than a minute on each. At the end of this browsing, he stayed on a page from a service with no age assurance in place for 1 minute and 35 seconds. The high number of pornography services visited within a short period, together with repeated searches and the presence of age gates on many of these services, suggests that the child may not have been able to access pornographic content on all of them and was instead trying multiple services to find one which would allow access.⁸²
- 4.32 Based on our analysis that aimed to replicate the experience of logged-out users, in May 2026, 33% of results on the first page of Google Search were to sites without protections⁸³ when searching for general porn-related queries. 90% of searches for general porn terms returned at least one site without protections. When searching for porn and circumvention queries, 15% of the results on the first page of Google were to sites without protections, while 78% of circumvention queries resulted in at least one site without protections being listed.
- 4.33 During similar Ofcom analysis in June 2026 that aimed to replicate the experience of logged-out users, we found 54% of results on the first page of Bing were to sites without protections when searching for general porn-related queries. 98% of searches for general

⁷⁸ The age assurance status of these services is correct as of May 2026.

⁷⁹ Ofcom, July 2026. Children's Passive Online Measurement (CPOM) – Pornography Services Report.

⁸⁰ The passive tracker used in Ofcom's CPOM study is unable to report on whether a visitor is logged into the site/app they are visiting or whether safe search setting is enabled.

⁸¹ Search engines accounted for around 30% of entry points overall.

⁸² Ofcom, July 2026. Children's Passive Online Measurement (CPOM) – Pornography Services Report.

⁸³ 'With protections' refers to services that are either age assured or geo-block UK users. 'Without protections' refers to services that do not appear to do either of those and as such display pornographic content without restrictions.

porn terms returned at least one site without protections. When searching for porn and circumvention queries, 39% of the results on the first page of Bing were to sites without protections, while 83% of circumvention queries resulted in at least one service without protections being listed.⁸⁴

- 4.34 Search services are not subject to the same duty as user-to-user services that requires them to use highly effective age assurance to prevent access to pornographic content by children, but the Act does put a duty on them to minimise children's exposure to this content.⁸⁵ When a user is inferred to be a child, we note Google and Bing default these users to settings with higher protections.
- 4.35 Following engagement with Google and Bing, they have agreed to work with Ofcom and other relevant stakeholders to explore practical solutions to address discoverability of porn services without protections via search engines. We welcome these efforts and encourage other search services and industry actors to work constructively with us to provide safer experiences for children.

The scale of services without age assurance creates significant risk to the effective use of age assurance on pornographic services

- 4.36 The presence of pornography services that do not have age assurance creates significant risk by enabling children to continue to access pornography services. Since January 2026, the number of services in the top 100 with age assurance in place has decreased steadily, as services without age assurance become more popular.⁸⁶
- 4.37 Our CPOM study found that nearly half of services visited by 8 to 14-year-olds had no age assurance in place.⁸⁷ Although relatively few children accessed these services, those who did visited multiple services without age assurance. A substantial share of overall visits were to services without age checks, indicating not only a gap in protections across the market, but also that children are finding such services.⁸⁸
- 4.38 As well as measuring children's experiences online, we used data from Similarweb to examine trends in traffic for a subset of 58 pornography services for which age assurance status is known.⁸⁹

⁸⁴ The findings from both Bing and Google are products of initial, early analysis. These findings should not be compared against each other due to methodological differences and the early nature of the analysis.

⁸⁵ Section 29(3) of the Act.

⁸⁶ Ofcom internal checks.

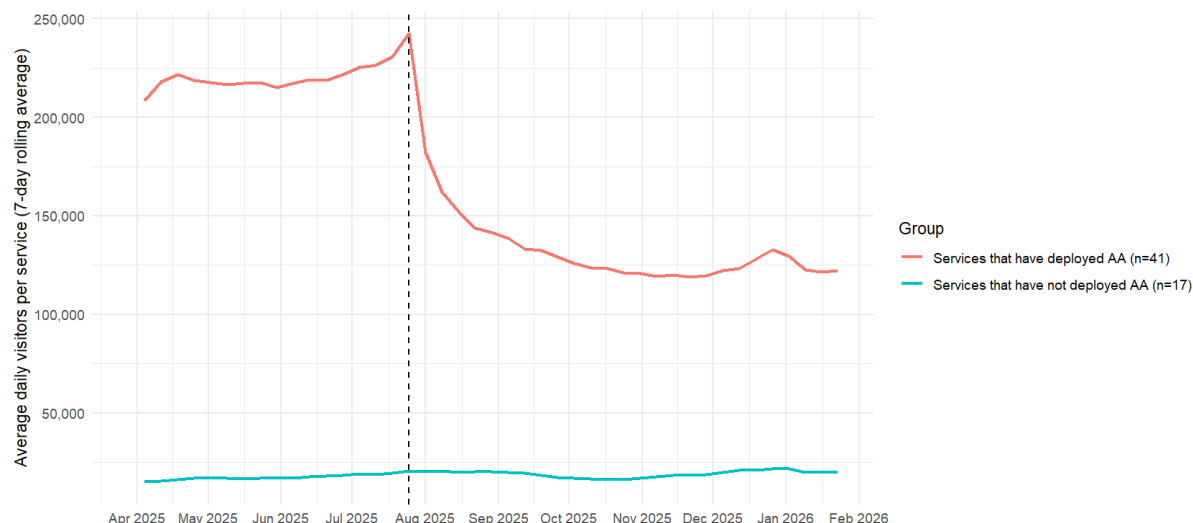
⁸⁷ Age assurance status correct as of May 2026.

⁸⁸ Ofcom, July 2026. Children's Passive Online Measurement (CPOM) – Pornography Services Report.

⁸⁹ We focused on a set of services that either implemented and retained age checks since 25 July 2025 (or shortly after) or that had not deployed them at any point as of April 2026. This is because user traffic is likely to vary conditional on implementation, but we do not always observe the timing of adoption. Including services for which age assurance status changed over time could therefore risk misclassification and affect the results. When identifying services with age assurance methods in place, no assessment was made regarding their effectiveness in the context of highly effective age assurance.

- 4.39 As shown in Figure 8, estimated average daily visitors for pornography services that deployed age checks in July 2025 fell sharply,⁹⁰ while trends for services that have never implemented age checks remained broadly stable over time.

Figure 8: Estimated average daily visitors per service by age assurance status



Source: Similarweb. 58 pornography services analysed from April 2025 to January 2026. Data extracted on 12 March 2026

- 4.40 We found considerable variation in traffic among services without age assurance, with 10 out of 17 services we analysed experiencing increases in estimated traffic. In some cases, these changes were substantial.⁹¹ For example, one service saw estimated average daily visitors increase from nearly 10,000 to around 25,000.⁹²
- 4.41 The observed decline in traffic following the introduction of age assurance is likely driven by a combination of factors, including migration to services with no age checks, users choosing to use fewer age assured sites⁹³, or some VPN use that is not captured in the Similarweb data.
- 4.42 The migration of users to services with no age checks in place is consistent with evidence from the US. In response to our 2025 CfE, the British and Irish Law Education Technology Association (BILETA) cited research in the US that has traced user behaviour following implementation of age assurance, which shows that while “it may have reduced search

⁹⁰ Similarweb defines daily visitors as the average number of individuals who visited the analysed website in one day. This metric is not deduplicated. An individual may be counted multiple times if they access a service from more than one device or visit multiple services in a given day. As such, the metric shown in Figure 8 may overstate the number of distinct users and should be interpreted as indicative of average service-level activity rather than unique individuals.

⁹¹ As mentioned above, the analysis focused only on a subset of services for which age assurance status was known and remained constant over time. This implies that a wider set of services may have experienced similar or potentially larger increases in user traffic.

⁹² The increases we observed across these services ranged from approximately 8% to 365%, depending on the service, with the highest percentage increases driven by those with very low traffic levels before 25 July 2025.

⁹³ Research indicates a reluctance to share personal data as a key barrier to use of age assured pornographic content sites, and evidence from Lucy Faithful Foundation indicates that some porn users are consuming less content since age assurance came into effect – which may include reference to use of fewer sites, lower frequency or less time spent.

traffic to regulated services, it has inadvertently strengthened the market position of non-compliant firms”. BILETA stated that this migration towards non-compliant services can result in users accessing sites with pirated or illegal content.⁹⁴ Other US research finds similar effects based on observed visits to the sites themselves, rather than search activity, showing that users shifted from services with age assurance to those with no age checks in place.^{95 96}

- 4.43 In response to our 2025 CfE, several stakeholders highlighted the risk that prescriptive age assurance on services could drive users toward unregulated or unsafe services.⁹⁷ One stakeholder noted that the perceived intrusiveness of methods of age assurance that are capable of being highly effective may deter engagement with “regulated services”, especially where there may be less incentive to complete age assurance processes, which risks pushing users towards “unregulated services”.⁹⁸
- 4.44 The observed migration of users towards services that do not have age assurance raises the risk that children could still be exposed to harmful content and points to user migration as a factor that risks preventing or hindering the effectiveness of age assurance. The financial impact of user migration is explored in Section 7.
- 4.45 Overall, our findings indicate that age assurance is proving effective at the individual service level when deployed correctly and in line with our HEAA guidance, but not yet at an overall sector level, due to user migration to non-age assured sites.
- 4.46 Enforcement remains a top priority for us. We are analysing thousands of adult services active in the UK to understand user migration and the popularity of the services, including emerging services with rising popularity. We are identifying non-compliant services and taking appropriate action. So far, we have opened 23 investigations into the providers of 88 adult services, resulting in the majority of services (73%) either implementing age assurance or blocking UK users. We have fined 7 providers of 24 sites so far – 8579 LLC (£1.35m), AVS Group Ltd (£1m), Kick Online Entertainment S.A. (£800k), the provider of fapello.com (£600k), Youngtek Solutions Ltd (£500k), First Time Videos LLC (£80k) and Itai Tech Ltd (£50k). Enforcement has prioritised action against providers based on the risk of harm posed by the services, including focusing on services who are growing their user numbers as a result of failure to put age checks in place. When it comes to deciding how to calculate the level of a penalty in cases where we find a breach, we consider (among other factors) the seriousness and duration of the non-compliance and the extent to which they have benefitted commercially from the breach.⁹⁹

⁹⁴ BILETA response to our 2025 CfE, p.7 (citing Lang, D.N., Listyg, B., Ross, B.V., Musquera, A.V. and Sanderson, Z. (2023) [Do Age-Verification Bills Change Search Behavior? A Pre-Registered Synthetic Control Multiverse](#)).

⁹⁵ Agarwal, S., Ananthakrishnan, U.M., Madio, L., Mitchell, M.F., Quinn, M., Reggiani, C. (2026) [Are you 18? Age Verification and Adult-Only Consumption in the US](#).

⁹⁶ Brown, M., Davis, E.J., Pope, D.G. (2026) [Can Online Activity Be Regulated? Evidence From Adult Websites](#).

⁹⁷ British and Irish Law Education Technology Association (BILETA) response to our 2025 CfE, pp. 7-8; [§<] response to our 2025 CfE, p.6; Association for UK Interactive Entertainment (Ukie) response to our 2025 CfE, p.7.

⁹⁸ Ukie response to our 2025 CfE, p.7.

⁹⁹ More information on our approach to enforcement can be found in Ofcom’s [Online Safety Enforcement Guidance](#) and [Penalty Guidelines](#).

- 4.47 While we are clear that the compliance obligations rest on regulated services themselves, protection of children requires a system-wide effort and more action is needed. To increase effectiveness and strengthen protections for children, there are questions about the role that other actors in the ecosystem can, and should, play, including search engines and operating systems. We welcome innovation in this space, while also emphasising the importance of ensuring that all interventions work effectively and reliably in practice, and regulated services can demonstrate that they have met their duties.

5. Social media services

Key findings

- Social media services typically use age assurance **to tailor children’s online experience**, rather than to prevent child access. The analysed social media services used two broad approaches to age assurance implementation:
 - **Active age gated content approach**, where only users attempting to access specific content, functionalities or parts of the service unsuitable for children are required to complete an age check; and
 - **Passive age inference approach**, where services 1) ask users to declare their age and then 2) apply age prediction models to subsequently infer whether a user is an adult or a child.

Overall, our research shows that children in the UK continued to be exposed to harmful content across social media services in the months following the children’s safety duties coming into force.

- **In particular, evidence suggests variability in the capability of age inference models, which reinforces our longstanding concerns about their efficacy.** In some cases, services may have failed to detect a significant proportion of child users.
- **Services using age inference models to comply with their child protection duties must be able to evidence that it is highly effective**, or switch to methods capable of being highly effective.
- To prevent children from encountering content harmful to children online, **we expect all social media services to fully implement relevant highly effective age assurance measures**, and to be able to demonstrate that these are effective in protecting children.

Age check implementation on social media services

- 5.1 Social media services are generally designed to be used by both adults and children. As a result, on social media services, age assurance is typically used to tailor the experience that a child receives, rather than to prevent all children from accessing the service as is the case in pornography services.
- 5.2 Any age assurance should work alongside other safety measures on social media services – content moderation, content recommender systems and user tools measures – to protect children from content harmful to children. In paragraph 5.14, we outline the need for highly effective age assurance, working in concert with other protections.
- 5.3 Across the analysed social media services, we observed two broad approaches to implementation:

- **An active age gated content approach**, whereby users can generally access and use the service without completing an age check.¹⁰⁰ A user only needs to actively complete an age check when attempting to access specific content, functionalities, or parts of the service that are reserved for adult users. This may include labelled content categories, channels, or communities.
- **A passive age inference approach**, whereby users declare their age upon access and age inference models are used to subsequently infer whether a user is an adult or a child, by analysing the user's activity on the service. Age inference is not included in our non-exhaustive list of methods that are capable of being highly effective in our HEAA guidance.¹⁰¹

Some services use age assurance at the point of access to harmful content which reduces the number of users who need to undergo age checks

- 5.4 In our age assurance measures and HEAA guidance, we state that services not dedicated to content harmful to children have flexibility to implement age assurance in a way that is most appropriate for the nature and design of their service. For example, service providers can choose to only require users to complete an age check if they wish to access content that the service has restricted to adult users rather than requiring all users to complete an age check at the point of entry. We refer to this as an active age gated content approach.
- 5.5 Five of the social media services that we analysed used this approach.¹⁰² Services stated that they chose this approach in light of privacy considerations, including minimising data collection. As shown in Figure 9, social media services using this approach had a low proportion of their user base that completed an age check, as expected.¹⁰³

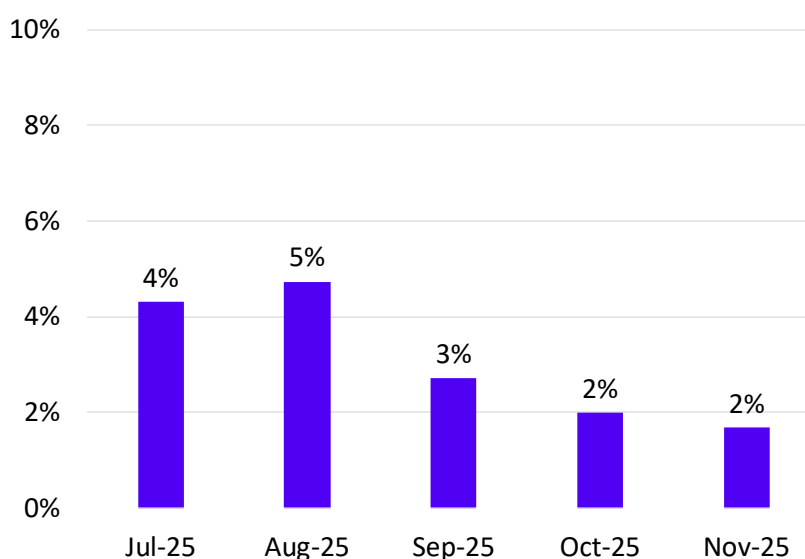
¹⁰⁰ We note that these services tend to also require users to declare their age at account creation, however this is usually separate to their age assurance process whereby users are typically required to complete an active age check to access harmful content.

¹⁰¹ Volume 4: 13.345-13.357. We made it clear that age inference is not capable of preventing children from accessing services whose principal purpose is the hosting or dissemination of PPC or PC as age inference requires the child to be active on the service for a period of time before an inference can be made. We recognised that age inference may be a component in a wider age assurance process, but noted that if providers wish to rely on it, they should evidence how it is technically accurate and robust in detecting a significant proportion of children (and the length of time taken) so that children are protected during this period.

¹⁰² [3<] 5 analysed services' responses to our information notices issued 15 December 2025. As well as actively age gating content, one of these services reported first using additional signals where available to determine if a user is an adult, such as whether an account had previously undergone photo ID verification or had been created prior to 2012 [3<]. These signals can be seen as passive.

¹⁰³ [3<] 5 analysed services' responses to our information notices issued 15 December 2025.

Figure 9: Proportion of active UK users who completed age checks per month for analysed services that actively age gate harmful content.



Source: Data from analysed services' responses to our information notice issued 15 December 2025.

- 5.6 Social media services that adopt an active age-gated content approach tended to deploy age assurance methods listed in our HEAA guidance as capable of being highly effective.¹⁰⁴ On average, these services offered users a choice of two methods.
- 5.7 Facial age estimation was offered by all five analysed services using an active age-gated content approach.¹⁰⁵ Three of them also offered photo ID matching.¹⁰⁶ This is consistent with the wider pattern observed across all service types, where facial age estimation was the most offered method. One social media service that adopted this approach also implemented additional methods listed in our HEAA guidance as capable of being highly effective, as well as using additional signals, such as whether an account had previously undergone ID verification or had been created prior to 2012.¹⁰⁷
- 5.8 Four out of five of the analysed social media services in question used facial age estimation without implementing a challenge age approach.¹⁰⁸ As highlighted in paragraph 4.11, we have made clear we think services should implement a challenge age where technically feasible to improve the overall effectiveness of the age assurance process by preventing or minimising borderline cases where the age estimation method incorrectly assesses a user's age. More information on this is given in Section 8.
- 5.9 Two of the five analysed social media services used proprietary age assurance technology¹⁰⁹ with one of these services using a combination of proprietary technology and third-party

¹⁰⁴ [3<] 5 analysed services' responses to our information notices issued 15 December 2025.

¹⁰⁵ [3<] 5 analysed services' responses to our information notices issued 15 December 2025.

¹⁰⁶ [3<] 3 analysed services' responses to our information notices issued 15 December 2025.

¹⁰⁷ [3<] response to our information notice issued 15 December 2025.

¹⁰⁸ [3<] 4 analysed services' responses to our information notices issued 15 December 2025.

¹⁰⁹ [3<] 2 analysed services' responses to our information notices issued 15 December 2025.

methods.¹¹⁰ The remaining services relied exclusively on third-party age assurance providers.¹¹¹

Some services rely on age inference models to detect and apply protections to child users

- 5.10 Four analysed social media services used age inference as the first layer of their age-assurance approach, which we did not include in the non-exhaustive list of methods set out in our HEAA guidance.¹¹² We refer to behavioural age inference models as “passive” because they analyse users’ activity on the service to infer their age, rather than users actively undergoing an age check (such as via facial age estimation or photo ID matching). The age inference models on all four services were developed by the service itself and based on proprietary technology.¹¹³
- 5.11 For this approach, following self-declaration of age upon accessing the service, services then use a range of signals and statistical/machine-learning models to infer the user’s age on an ongoing basis. These signals include measurements of a user’s activity or behavioural indicators, and account-level information.
- 5.12 All of these services outlined that they may trigger additional types of age checks where there is low confidence in a user’s age, or where specific risk signals are detected.¹¹⁴ This may occur, for example, where a user attempts to access age-restricted content, displays behaviour inconsistent with their stated or inferred age, or attempts changes to age-related account settings. In these cases, users are asked to confirm their age using methods including facial age estimation, photo ID matching, credit card checks or email-based age estimation. Where additional checks were triggered, services typically offered users multiple options to choose from to prove their age, most of which were delivered by third-party providers.
- 5.13 Social media services taking a passive age inference approach claimed that it enables the provision of service-wide age-appropriate experiences. They also emphasised privacy and proportionality considerations in choosing this approach, which are considered in more detail in Section 7.

Effectiveness of age assurance for social media services

- 5.14 Knowing if a user is a child is a necessary step in ensuring that children are protected and not exposed to harmful content on social media. Services also need to implement effective content moderation to consistently identify and detect content harmful to children. Additionally, services need to ensure that their content recommender systems do not push content identified as harmful to children. Age assurance, content moderation and the

¹¹⁰ [redacted] response to our information notice issued 15 December 2025.

¹¹¹ [redacted] 3 analysed services’ responses to our information notices issued 15 December 2025.

¹¹² [redacted] 4 analysed services’ responses to our information notices issued 15 December 2025. These services typically had a range of systems and processes in place to protect children before the age assurance duties came into force in July 2025.

¹¹³ [redacted] 4 analysed services’ responses to our information notices issued 15 December 2025.

¹¹⁴ [redacted] 4 analysed services’ responses to our information notices issued 15 December 2025.

design of content recommender systems work jointly to reduce children’s exposure to harmful content and each of these processes needs to be effective.¹¹⁵

- 5.15 On services that take an active age-gated content approach, the content that they are restricting access to should be placed behind an age gate, and any user that has not completed an age check and been determined to be an adult should not be able to see it.
- 5.16 On services that use a passive age inference approach, service providers must apply protections and/or restrict access to harmful content for all users that they have not determined to be adults. This includes all users that the age inference models determine as children, as well as any users for whom the age inference models have not yet made a determination either way (even where users may have self-declared as over 18). Services relying on behavioural age inference should have high levels of confidence that the model is effective at determining if a user is a child or an adult.
- 5.17 We have examined a range of evidence, including our own research and data gathered via information notices, to consider the extent to which services are meeting these outcomes through their use of age assurance. We have identified areas for improvement by industry in Section 8.

Evidence suggests there have been minimal changes to children’s overall online experiences across social media services

- 5.18 As reported in our [Children’s Online Experiences report](#), our recent research suggests there has been limited change in children’s exposure to harmful content¹¹⁶ online since the children’s safety duties came into force.
- 5.19 Wave 2 of COST,¹¹⁷ published in May 2026, found that 73% of children aged 11 to 17 recalled exposure to at least one piece of harmful content in the four weeks before the survey. This is broadly consistent with Wave 1 results from March 2025 to April 2025, where the equivalent figure was 70%.¹¹⁸ This suggests little change in recalled exposure to harmful content following the children’s safety duties coming into force. The services children are most likely to mention when asked about their exposure to harmful content tend to reflect the popularity of those services among children.¹¹⁹

¹¹⁵ Ofcom, 2025. Statement: Protecting children from harms online, Volume 4.

¹¹⁶ In the context of the children’s online experiences research report, which draws on findings from COST, the term “harmful content” is used to refer collectively to PPC and PC only – it does not include exposure to non-designated content (NDC). Measurement of children’s exposure to NDC was introduced at Wave 2 of COST. As a result, trend analysis between Wave 1 and Wave 2 is limited to children’s exposure to PPC and PC only. Children were not shown harmful content but were prompted with a list of examples of harmful content, see Children’s Online Experiences Report annex for definitions.

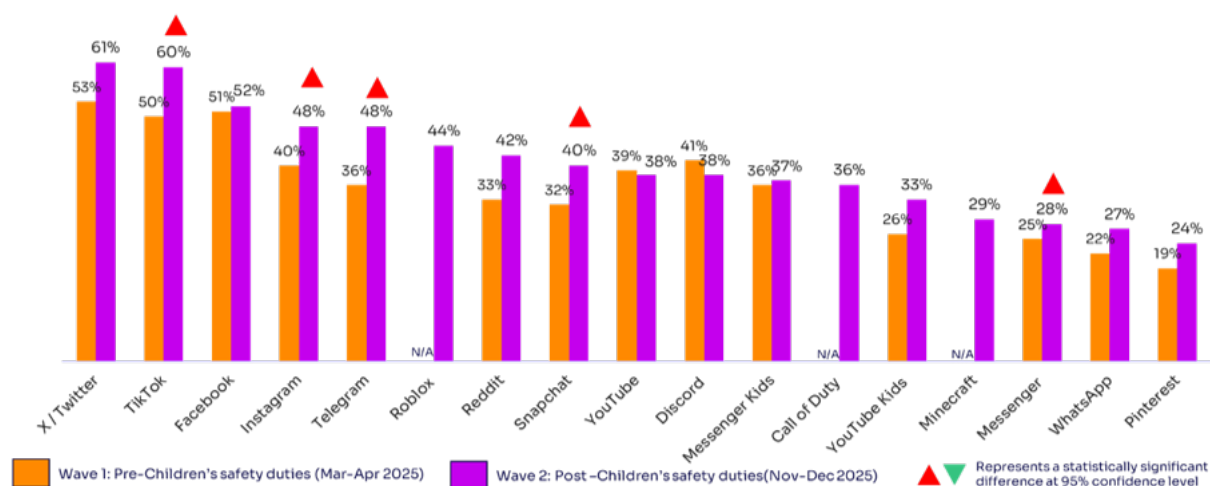
¹¹⁷ Ofcom, 2026. Children’s Online Safety Tracker. The term “wave” refers to a specific round of data collection. Wave 1 fieldwork was conducted before the implementation of age assurance (March 2025 to April 2025), while Wave 2 occurred four months after its implementation (November 2025 to December 2025).

¹¹⁸ Ofcom, 2026. Children’s Online Safety Tracker.

¹¹⁹ For full detail of these findings please see the Children’s Online Experiences Report, pages 21-23.

5.20 We have also assessed recalled exposure to harmful content among child users¹²⁰ of specific online services, including social media services. Looking at data from children who say they use these services and examining the proportion who say they were exposed to harmful content while using that service, highlights which services may be more likely to expose their users to harmful content, regardless of how widely they are currently used. As shown in Figure 10, across some services a growing share of child users said they had seen harmful content at Wave 2.¹²¹

Figure 10: 11 to 17-year-olds' recalled exposure to harmful content among child users of services



Source: Ofcom, 2026. Children's Online Safety Tracker. This data was first published in May 2026 and includes services analysed in the age assurance report and services that are not included in the scope of the report.

5.21 Our survey on children's experiences of being asked to verify their age¹²² was conducted among 8 to 17-year-olds who had at least one profile on a social media site that we asked about.¹²³ The survey showed that while 56% of children reported noticing changes to their online experiences since July 2025, only 11% reported not being able to access content or features they previously could,¹²⁴ and 16% saw less upsetting or inappropriate content online.¹²⁵ Therefore, while a majority of these children reported noticing some sort of change to their online experience, only a minority reported having noticed changes that are more directly related to age assurance.¹²⁶

¹²⁰ "Child users" refer to children aged 11 to 17 who use online services and said they had used the service in the four weeks prior to fieldwork.

¹²¹ Ofcom, 2026. Children's Online Safety Tracker.

¹²² Ofcom, 2026. Children's experiences of being asked to verify their age. Waves 3 and 4 combined.

¹²³ The sites and apps about which we asked were Facebook; YouTube (not including YouTube Kids); Snapchat; Instagram; TikTok; X; Discord; Pinterest; Twitch; Reddit; Roblox, and Other (please specify).

¹²⁴ Full response: I can't use something I could before (for example, I can't use some parts of an app/website like livestreaming, watch something online or use an app/website).

¹²⁵ Full response: I've seen less upsetting or inappropriate stuff online (For example, violent or scary videos, dangerous stunts/challenges, or things that might make people feel bad about how they look).

¹²⁶ Notably, where children have not noticed changes, it does not mean the changes have not happened as some processes and changes, such as age inference, may be less visible to child users. Changes to service

- 5.22 Thirdly, our Parents’ Perceptions of Protection of Children Measures Study suggests that UK parents observed little change in their children’s online experiences.¹²⁷ In October 2025, 11% of UK parents reported that during the previous three months their children were no longer able to access certain content, platforms or features they previously could. Similar proportions said their children had been asked to complete an age check online (10%) and / or had encountered less inappropriate content (9%).¹²⁸
- 5.23 Taken together, only a minority of children and parents reported age assurance related changes to the children’s online experiences since the children’s safety duties came into force. However, it is worth noting that these early findings rely on self-reported experiences of changes with interviewees that may have missed less visible changes, particularly where services use approaches that rely on passive age inference models.¹²⁹
- 5.24 Some stakeholder responses to our 2025 CfE are consistent with these findings. For example, Internet Matters reported that children aged 9 to 17 in the UK continue to encounter harmful content,¹³⁰ with only modest reductions across most categories and an increase in pornographic content exposure.¹³¹ The UK Safer Internet Centre said 24% of Report Harmful Content cases involved users under 18, which they said showed that harmful content persists on platforms with weak age verification and minimal moderation.¹³²
- 5.25 There are several possible reasons why reported exposure to harmful content may not have fallen materially yet, for example: (1) age assurance processes may not consistently determine the age of all children accurately; (2) some children may circumvent age checks to access restricted content or bypass age checks altogether (for example, using VPNs)¹³³; (3) harmful content may be encountered before protections are applied;¹³⁴ (4) content moderation systems may fail to consistently and accurately identify harmful content; and (5) content recommender systems may not restrict or reduce the visibility of such content in children’s feeds.¹³⁵
- 5.26 While exposure to harmful content (as defined in the Act) may not have declined significantly overall, there are signs of improvement at platform level for PPC across some services. Consistent with this, we saw a reduction in 11 to 17s saying they had been exposed to content (in a four-week period) on an app, website or online game that *they*

features and functionalities may also not have been relevant for children due to the user not being exposed to harms, or due to already having been determined to be a child and were subject to existing safeguards.

¹²⁷ Ofcom, May 2026. Parents’ Perceptions of Protection of Children Measures Study.

¹²⁸ While there are limitations with relying on parents’ knowledge and perceptions of their children’s online experiences, the fact that both parents and children reported changes to the children’s experiences at similar levels gives us greater confidence in these findings.

¹²⁹ It is also possible that children would not experience any change if they had already been determined as a child and were subject to existing safeguards on services prior to July 2025.

¹³⁰ We note that the categorisation of harmful content by Internet Matters does differ to how we define and assess harmful content for our COST research.

¹³¹ Internet Matters response to our 2025 CfE, p.3.

¹³² UK Safer Internet Centre response to our 2025 CfE, p.4.

¹³³ See paragraph 7.66-7.74 where we consider use of VPNs.

¹³⁴ For example, this could occur for some services that use age inference in the instance that a child has falsely self-declared as over 18.

¹³⁵ Evidence from our Children’s Online Safety Tracker shows content recommender systems as the most frequent pathway for exposure to harmful content.

considered inappropriate, and that made them feel upset, scared or uncomfortable.¹³⁶ Therefore, there are some positive indicators within the evidence base, despite overall exposure to harmful content remaining stable, or in some cases increasing.

- 5.27 It is worth highlighting that the Act only requires services to use highly effective age assurance to prevent children from accessing PPC where their terms of service do not prohibit one or more kinds of PPC. The Act does not require the use of age assurance for PC and/or NDC, however we have recommended in our measures that services should use highly effective age assurance to meet their duties regarding PC and/or NDC where they also allow this kind of content.
- 5.28 In summary, while the evidence outlined in this section does not establish causation, taken together, it suggests that the current age assurance processes in combination with other children's safety measures (such as content moderation measures, as outlined in paragraph 5.14) taken by social media services are not yet delivering the intended outcome of effectively protecting children from encountering harmful content.

Analysis of age inference models suggests variance in capability

- 5.29 We have gathered and analysed evidence about the capability of age inference models to successfully determine whether a user is an adult or a child.
- 5.30 In our [January 2025 Statement on Age Assurance and Child Access](#), we set out our position that age inference was not a method capable of being highly effective for services that are dedicated to content that is harmful to children (e.g. pornography services) who need to implement highly effective age assurance to prevent children from accessing the entire service. This is because age inference models, by design, require children to be on the service for a period of time for an inference to be made. Therefore, these services could not reasonably implement age inference models to comply with their duties to prevent children from encountering content harmful to children.
- 5.31 We acknowledged that age inference could, in theory, play a role for services that children are allowed to access, but must be protected from harmful content that may be present on the service. However, in our April 2025 Statement, we decided not to add age inference to the non-exhaustive list of kinds of age assurance that we consider are capable of being highly effective, due to insufficient evidence and concerns over its efficacy.¹³⁷
- 5.32 Since publishing our April 2025 Statement, the ICO has updated its position on the use of age inference (also known as profiling for age assurance).¹³⁸ They consider that services can use it as an anti-circumvention tool to identify under 13s who have slipped through robust age gates, where they can demonstrate the necessity and proportionality of their approach and the effectiveness of their model. However, the ICO considers that it is not appropriate

¹³⁶ Exposure to content that children aged 11 to 17 had seen or heard something inappropriate on an app, website or online game that made them upset, scared or uncomfortable fell from 29% in Wave 1 to 24% in Wave 2 of the Children's Online Safety Tracker. When prompted with a list of harmful content types, as defined in the Act, exposure remained constant from Wave 1 to Wave 2 (70% Wave 1, 73% Wave 2).

¹³⁷ Volume 4, paragraph 13.355-13.357.

¹³⁸ ICO, 2025. [Annex: What we've learned about profiling for age assurance](#).

to use profiling to make up for a weak or non-existent age gate if under 13s are not permitted on a service.

- 5.33 In our April 2025 Statement, we stated that if service providers wished to implement age inference, they should consider how best to evidence how their methods are technically accurate and robust at detecting a significant proportion of children, the length of time different age inference models take to determine whether a particular user is an adult or a child and how children are protected during this period. We also outlined how they could evidence reliability and fairness, as well as the consideration they should give to user privacy and the processing of children’s personal data under the data protection regime.¹³⁹
- 5.34 As part of this report, we have analysed the extent to which the age inference models currently deployed by four social media services included in this report achieve this outcome, by considering how the number of users to whom these services are applying child protection measures aligns with Ofcom’s evidence-based estimates of the number of child users on those services.
- 5.35 To do this, we requested information from the services that rely on age inference models about the number of users that they apply their child protection measures to, as a proxy for the number of users that the service determines to be a child. We calculated our own estimates of the number of children that use these services by triangulating multiple sources. We then compared services’ figures with our estimates, to assess whether service providers are applying their child protection measures to a similar proportion of children that claim to use the services. Throughout this process, we exercised caution to ensure that the comparisons were carried out as accurately and consistently as possible, providing opportunities for each service to clarify their approach and the data provided.
- 5.36 Our analysis indicates that the proportion of child users based on services’ figures did not consistently align with our own estimates and in some cases, were consistently lower. The most significant methodological factor that may account for at least part of these differences is Ofcom’s estimates capture logged-in and logged-out users, whereas the figures provided by services generally related to accounts on the platforms only.¹⁴⁰
- 5.37 However, where we consistently observed significant differences between services’ figures and our own estimates, this may indicate that, despite any methodological differences, some services may have failed to detect a significant proportion of child users on their platforms. This could in turn suggest that their approach to age assurance is not able to determine whether a user on their platform is a child, which could put child users at risk of harm. We are engaging with services as a matter of priority on this analysis.
- 5.38 Our findings reinforce our long-standing serious concerns about the efficacy of these age inference models. Services that use age inference should replace or supplement it with other method(s) of age assurance that our HEAA guidance states are capable of being highly

¹³⁹ Volume 4, paragraph 13.355 – 13.357.

¹⁴⁰ It should be noted that two of the four services in question [X] explained that any logged-out user is restricted from accessing sensitive, inappropriate, or harmful content on their service, which should mean that the ability to protect logged-out child users from such content is not dependent on the services’ ability to detect them as children.

effective, unless they can demonstrate using reliable evidence that it is highly effective and meets UK data protection obligations.

6. Dating services

Key findings

- Analysed dating services operating in the UK have deployed age assurance to enforce their minimum age of 18, to **prevent children from accessing their services**.
- They implemented methods from our list of methods capable of being highly effective, but offered limited choice, with most services relying on **facial age estimation without a challenge age**.
- We observed that **just over one in ten 15 to 17-year-olds were visiting and spending time on the three highest-reaching dating apps** in December 2025, whereas 8 to 14-year-olds generally do not seem to visit these apps. This indicates that age assurance was unlikely to be completely preventing child access at this time.
- Our analysis therefore suggests that the age assurance processes that analysed dating services were using in December 2025 required improvement. We note that these services have begun to take steps to improve their age assurance process since they responded to our information notices.

Age check volume and implementation on dating services

- 6.1 Since the children’s safety duties came into force, some online dating services have implemented age checks. The decision of dating sites to implement age assurance to protect children from harmful content depends on the context and risks to children of the service in question, including whether harmful content is allowed in their terms of service. Some services (such as those that allow users to share intimate images) are required under the Act to implement highly effective age assurance to comply with the children’s safety duties, whereas others have proactively chosen to implement age assurance to enforce a minimum age requirement of 18.
- 6.2 The four dating services analysed for the purpose of this report use age assurance to prevent children from accessing the entire service.¹⁴¹ This means that active UK users should only be able to access the service once they have completed an age check and been determined as an adult.
- 6.3 Analysed dating services used methods set out in our HEAA guidance, with all four services implementing facial age estimation and photo ID matching.¹⁴² For three of these services, most users would only be presented with the option of facial age estimation,¹⁴³ with photo ID matching reserved for specific instances, such as where users had self-declared as under

¹⁴¹ [3<] 4 analysed services’ responses to our information notices issued 15 December 2025.

¹⁴² [3<] 4 analysed services’ responses to our information notices issued 15 December 2025.

¹⁴³ [3<] 3 analysed services’ responses to our information notices issued 15 December 2025.

18 and wanted to gain access, or for users who were appealing the result of facial age estimation.

- 6.4 Two of the four services used liveness detection technology to help mitigate the risk of circumvention by children,¹⁴⁴ while the other two did not have liveness detection in place at the time.¹⁴⁵ As set out in our HEAA guidance, any service that uses facial age estimation or photo ID matching should deploy liveness detection because it can help reduce the risk of children using still images of adults to circumvent these methods. Section 8 highlights this as a key area where services can improve their process.
- 6.5 Multiple analysed dating services deployed facial age estimation without a challenge age at the time of responding to the information notices.¹⁴⁶ As highlighted in Section 8, we urge services to implement a challenge age approach where technically feasible. This will improve the overall effectiveness of the age assurance process by reducing borderline cases in which facial age estimation may incorrectly assess a user's age.
- 6.6 In the months since we collected the data for this report, the analysed dating services referenced in this report have begun taking steps to improve their age assurance processes as a result of Ofcom engagement. This includes introducing challenge age approaches and liveness detection.
- 6.7 Analysed dating services reported that they used user reporting¹⁴⁷ and/or automated detection¹⁴⁸ to retrospectively detect users who are under 18 but had managed to pass the initial age check to gain access to the service. These users are then removed from the service.

Effectiveness of age assurance for dating services

- 6.8 For the use of age assurance to be effective on analysed dating services, it must prevent children from accessing the service altogether. In practice, we would expect to observe a decline in the number of children accessing these dating services and the time spent on these services.
- 6.9 The evidence available to us at this early stage suggests that in December 2025, some older teenagers were still visiting and spending time on analysed dating sites. While we note that this data was collected before the improvements outlined in paragraph 6.6, it indicates that in December 2025 age assurance processes were unlikely to be effective at preventing access to dating services for some older teenagers.

¹⁴⁴ [3<] 2 analysed services' responses to our information notices issued 15 December 2025.

¹⁴⁵ [3<] 2 analysed services' responses to our information notices issued 15 December 2025.

¹⁴⁶ [3<] 4 analysed services' responses to our information notices issued 15 December 2025.

¹⁴⁷ [3<] 4 analysed services' responses to our information notices issued 15 December 2025.

¹⁴⁸ [3<] 3 analysed services' responses to our information notices issued 15 December 2025.

Over one in ten 15 to 17-year-olds were still visiting and spending time on dating services five months after the children's safety duties came into force

- 6.10 An Ofcom study did not find evidence that significant numbers of 8 to 14-year-olds are visiting the three highest reaching dating apps.¹⁴⁹ However, data from Ipsos Iris indicated that in December 2025, 12% of UK online 15 to 17-year-olds visited at least one of the three highest reaching dating apps. This remains comparable to the 12% reported in May 2025 before the children's safety duties came into force in July 2025.¹⁵⁰
- 6.11 The average time spent in December, calculated per visitor at an individual service level, ranged from 1 to 4 hours.¹⁵¹ This suggests that there are 15 to 17-year-olds attempting to access dating services. The average time spent suggests that they may, in some cases, be succeeding.

Information notice data indicates that a very low proportion of users are subsequently flagged as children after the initial age check

- 6.12 Evidence collected via information notice showed that under 0.04% of users who completed an age check across the analysed services were later identified as under 18 through user reporting¹⁵² and/or automated detection¹⁵³ between July to November 2025. While this could indicate robustness of the original age check resulting in very few children accessing the services, in light of the evidence outlined in paragraph 6.10 and 6.11, it could also suggest that child users who are granted access to these dating services are rarely detected and removed afterwards.
- 6.13 Taken together, the research findings and information notice data underline the importance of dating services using highly effective age assurance. It is clear that there is intent among children, and in particular older teenagers, to access these services. For dating services to robustly enforce their minimum age limits of 18, it is vital that they use methods that are capable of being highly effective and take the right steps (such as using a challenge age and liveness detection) to ensure that these methods are highly effective in practice.

¹⁴⁹ Ofcom, 2026. Children's Passive Online Measurement Study, fieldwork October 2025 to March 2026.

¹⁵⁰ Ipsos, Ipsos iris online measurement service, app only, May and December 2025, internet users aged 15 to 17, UK. Base: 193 in May and 118 in December 2025.

¹⁵¹ Ipsos, Ipsos iris online measurement service, app only, May and December 2025, internet users aged 15 to 17, UK. Base: 193 in May and 118 in December 2025.

¹⁵² [3] 4 analysed services' responses to our information notices issued 15 December 2025.

¹⁵³ [3] 3 analysed services' responses to our information notices issued 15 December 2025.

7. Factors that have prevented or hindered the effective use of age assurance

Key findings

- Evidence from analysed services indicates that the **direct costs of implementing age assurance do not appear prohibitively high**. However, the evidence provided was incomplete across analysed services and other sources indicates that **costs could pose a barrier to smaller services**.
- Sharp declines in user traffic on pornography services with age assurance point to **revenue losses associated with the implementation of age assurance** and is consistent with evidence from multiple analysed services. The magnitude of these effects likely varies across services, depending on their reliance on advertising and the revenue potential of the remaining user base. However, the evidence on these service-specific factors is limited.
- Analysed services demonstrated **strong awareness of privacy requirements**, with data minimisation commonly shaping the design and implementation of age assurance processes. However, privacy remains a prominent concern about age assurance among UK users.
- **Circumvention appears low, with a relatively small minority of children reporting that they circumvent highly effective age checks or use VPNs to access restricted content or features**. However, some activity may not be captured due to reporting bias.

7.1 In this section, we consider whether there are factors that may have prevented or hindered the effective use of age assurance, or a particular kind of age assurance, for the purpose of services' compliance with their duties set out in the Act. In accordance with Section 157 of the Act, we must, in particular, consider whether the following have prevented or hindered the effective use of age assurance:

- The **cost** to providers of using it; and
- The need to protect users from a breach of any statutory provision or rule of law concerning **privacy** that is relevant to the use or operation of a regulated service (including, but not limited to, any such provision or rule concerning the processing of personal data).

7.2 In addition to the two factors set out above, the bypassing and circumvention¹⁵⁴ of age checks by children commonly appeared in our research. We therefore consider the extent to which this is preventing or hindering the effective use of age assurance.

¹⁵⁴ Where we discuss the bypassing of age checks, this refers to avoiding undergoing the age check for example by using a VPN or migrating to a service without age assurance. Circumvention refers to attempting to break or spoof the age check, which might include using a false identity document or a video avatar to complete the age check.

- 7.3 These factors are cross-cutting and apply to all service types discussed above. Where there are specific sector-level nuances, we have drawn this out.

Cost to providers

- 7.4 In this section, we review the available evidence on the direct and indirect costs of implementing and operating age assurance.¹⁵⁵ Direct costs refer to costs directly associated with a service implementing and operating age assurance, including set-up costs, ongoing costs and check costs where applicable. Indirect costs refer to the impact on service revenue driven by changes in user behaviour, following the implementation of age assurance.
- 7.5 Overall, the available evidence from the information notice responses suggest that direct costs of age assurance are unlikely to have been a major factor hindering the effectiveness of age assurance for the analysed service providers. However, there are some indications from other sources that costs may pose greater challenges for smaller services.
- 7.6 Evidence from the information notice responses and user traffic data suggests that indirect costs are a factor that appear to be hindering or preventing the effectiveness of age assurance. Sharp reductions in traffic to pornography services with age assurance point to revenue losses associated with its implementation, in line with evidence provided by multiple service providers. These effects appear to be more pronounced among free-to-access services and those that rely on advertising to large numbers of users, though evidence remains limited.

Direct costs do not appear to be prohibitively high, but the available evidence is limited

- 7.7 As discussed in Sections 3-6, analysed services have adopted different approaches to age assurance, including using third-party providers and in-house solutions (or both). This distinction is relevant for analysing costs.
- 7.8 Costs for third-party solutions are generally easier to identify, as, for example, they can involve discrete per-check payments. By contrast, costs for in-house systems are more difficult to estimate, as they are typically distributed across a range of engineering and operational activities.

Costs of implementing and operating a third-party solution

- 7.9 We asked analysed service providers using third-party age assurance solutions for information on:
- costs of setting up the solution (set-up costs);
 - costs of running the solution (ongoing costs); and
 - costs to check the user base (check costs).

Set-up costs

- 7.10 Where reported, set-up costs do not appear high for the analysed service providers, but evidence is limited. A minority of analysed service providers reported not incurring any set-

¹⁵⁵ We have reviewed evidence from the information notice and our 2025 CfE and have used Similarweb data to analyse changes in user traffic.

up costs,¹⁵⁶ typically reflecting pre-existing vendor relationship or prior deployments of age assurance in other jurisdictions rather than UK-specific development.¹⁵⁷ This does not rule out the possibility that these service providers still incurred opportunity costs through the diversion of resources. Where set-up costs were reported, figures largely clustered in the tens of thousands of pounds, with costs typically relating to internal IT integration, engineering work, testing and user support.¹⁵⁸ A small number of analysed service providers reported higher headline figures up to a few million pounds, but combined set-up and ongoing internal costs and were therefore not directly comparable.^{159 160}

- 7.11 However, not all of the analysed service providers were able to report set-up costs, particularly among social media services.¹⁶¹ Some of the analysed service providers cited this is due to time elapsed since roll-out and attribution challenges, as age assurance was implemented through shared resources and cross-functional teams.¹⁶² While this limits the extent to which we can assess the scale of set-up costs, the evidence available does not allow us to conclude they prevented the effective deployment of age assurance for the analysed service providers.

Ongoing costs

- 7.12 Many analysed service providers reported incurring ongoing costs associated with operating third-party age assurance solutions.¹⁶³ Where described, costs typically relate to product and engineering resourcing, operations and customer support, compliance and monitoring activities, and opportunity costs reflecting the diversion of resources from other priorities.¹⁶⁴
- 7.13 However, analysed service providers generally did not quantify these costs.¹⁶⁵ Some of the analysed service providers explained this is due to costs being embedded within wider business operations, making them difficult to isolate and report separately.^{166 167} While these costs may represent an additional cost for businesses and be relevant in some cases, the evidence we reviewed does not allow us to conclude they prevented the effective deployment of age assurance for the analysed service providers.

¹⁵⁶ [X] 5 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁵⁷ [X] 3 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁵⁸ [X] 5 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁵⁹ [X] 2 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁶⁰ The figures reported by these service providers included costs such as engineering efforts, supporting labour functions, external legal advice, and other contracted services. These service providers also reported operating at large scale, having already performed millions of age assurance checks since rollout.

¹⁶¹ [X] 6 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁶² [X] 2 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁶³ [X] 13 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁶⁴ [X] 10 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁶⁵ [X] 7 analysed service providers' responses to our information notices issued 15 December 2025.

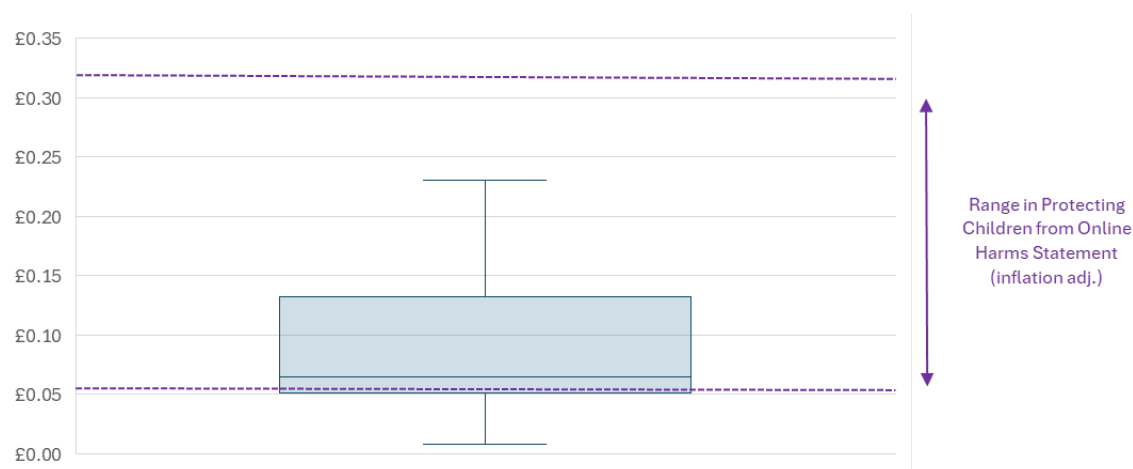
¹⁶⁶ [X] 3 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁶⁷ A small number of analysed service providers provided estimates for some of the ongoing costs they incurred, clustering in the tens of thousands of pounds [X<3 analysed service providers]. A few reported higher figures, but they either combined different cost categories or reflected global figures rather than UK-specific activity and were therefore not directly comparable [X<4 analysed service providers].

Per-check costs

7.14 The estimated average per-check cost for the analysed service providers to check users does not appear high. In our April 2025 Statement, we estimated per-check cost figures in the range of £0.05 to £0.30.¹⁶⁸ As shown in Figure 11, our estimates of the average per-check cost incurred by the analysed service providers had a median of around £0.06, with most estimates falling at or below £0.10.^{169 170} While a small number of analysed service providers reported higher costs, all estimates in our sample remained below the upper bound of £0.30.¹⁷¹ Annex 3 provides further detail on per-check cost by age assurance method incurred by the analysed service providers.

Figure 11: Distribution of estimated average per-check cost incurred by the analysed service providers¹⁷²



Source: Services' responses to our information notice issued 15 December 2025.

7.15 When interpreting per-check cost estimates, it is important to consider how third-party age assurance service providers set their prices. While only some of the analysed service providers shared pricing details, those that did revealed various commercial models, including fixed fees, subscriptions, and volume-tiered pricing. In these situations, per-check costs often represent average spending instead of a consistent price per check, and these costs may decrease as the number of checks increases.¹⁷³ This indicates that some service providers benefit from economies of scale, so performing more age checks does not always mean costs rise at the same rate.

¹⁶⁸ Volume 5 Annex. Paragraph A3.30, Page 9.

¹⁶⁹ [3<] 12 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁷⁰ Responses from most service providers we sent an information notice to include sufficient information to derive a cost-per-check figure (excluded from analysis for lack of data: [3<3 analysed service providers']. A minority of service providers explicitly stated the cost-per-check they get charged by their third-party providers; in all other cases, figures are calculated based on reported spend and check volumes.

¹⁷¹ [3<] 4 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁷² The box plot in the figure summarises how the average per-check costs are spread across the analysed services. The line inside the box shows the median, meaning half of the observations are above this value and half are below. The box borders show the middle half of observations, from the 25th to the 75th percentile. The whiskers show the lowest and highest observed costs.

¹⁷³ [3<] 6 analysed service providers' responses to our information notices issued 15 December 2025.

- 7.16 The impact of per-check costs may also vary depending on a service providers' operating model. Service providers that do not operate a signed-in model or that cannot reliably recognise returning users may need to conduct repeated checks for the same user over time. This could make per-check costs more material for some services, particularly where they operate at high user volumes and generate relatively low revenue per user.

Costs of building and operating an in-house solution

- 7.17 We asked analysed service providers using in-house solutions to provide information on:
- one-off/set-up costs; and
 - ongoing costs.
- 7.18 Evidence on in-house costs is limited and fragmented. Analysed service providers generally reported that they were unable to estimate costs comprehensively, citing challenges with internal cost tracking and attribution, and time elapsed since implementation.¹⁷⁴ Where figures were provided, they were reported on different bases (such as UK-specific versus global) and with varying levels of aggregation. This limits direct comparison across service providers but still provides some evidence on the broad scale and types of costs involved.
- 7.19 Reported set-up costs varied widely. Analysed service providers that gave UK-specific estimates indicated relatively low costs, typically in the tens of thousands of pounds, in some cases reflecting the use of existing in-house capabilities and limited incremental resourcing.¹⁷⁵ One service provider reported costs in the low millions, although this figure combines set-up and ongoing costs and includes both in-house and third-party elements.¹⁷⁶ At a global level, set-up costs can be more significant and involve engineering effort, dedicated staff, and infrastructure resources (such as data storage and cloud compute).¹⁷⁷
- 7.20 Analysed service providers were often unable to quantify ongoing costs of operating their in-house age assurance solutions.¹⁷⁸ A number of service providers reported global estimates, ranging from the tens to low hundreds of millions of pounds per year, covering costs such as ongoing staffing, infrastructure, data storage, cloud compute, and human review.^{179 180}

Direct cost constraints for smaller services

- 7.21 While the evidence from the analysed service providers suggests that costs of age assurance are unlikely to have been a major factor hindering the effectiveness of age assurance, other evidence suggests these costs may be more challenging for smaller services.
- 7.22 A number of respondents to our 2025 CfE – including services, age assurance vendors, trade associations and civil society organisations – raised concerns that these costs could place a

¹⁷⁴ [X] 4 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁷⁵ [X] 2 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁷⁶ [X] response to our information notice issued 15 December 2025.

¹⁷⁷ [X] response to our information notices issued 15 December 2025.

¹⁷⁸ [X] 3 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁷⁹ [X] 2 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁸⁰ While these figures may appear high in absolute terms, they appear to represent a small proportion of the annual turnover reported by these service providers.

disproportionate burden on smaller services.¹⁸¹ This evidence mainly reflected stakeholder views and was not generally quantified, although some respondents referred to direct business experience.¹⁸²

- 7.23 Some of these respondents pointed to costs including building or buying their own age assurance systems, ongoing operations, and technical or governance measures such as security, auditing, testing and model retraining.¹⁸³ Some said these costs could affect the quality of age assurance solutions adopted for some platforms, as well as investment, recruitment, innovation and commercial viability.¹⁸⁴ In some cases, respondents linked cost pressures to decisions to exit the market or block UK users.¹⁸⁵
- 7.24 This is consistent with the evidence discussed in Section 4, which shows that – at least for some pornography services – age assurance adoption rates decline steadily as the service popularity decreases. This could suggest that less popular services may face greater challenges in absorbing costs of deployment.
- 7.25 The impact of these costs may depend on a service’s business model. Based on our direct engagement with services as part of our supervision activity, for example, costs of age assurance in the pornography sector may be more of a barrier for free-to-access cam sites and video-sharing platforms (tube sites), compared to premium services such as subscription-based or paid-access platforms.
- 7.26 First, age assurance set-up and ongoing costs may represent a higher share of operational costs for free-to-access cam services and tube services, as they generally do not require extensive technical infrastructure to operate. By contrast, premium services typically already maintain a technical infrastructure (for example to process payments, manage accounts and engage with content providers), reducing the relative impact of integrating age assurance.
- 7.27 Second, per-check costs can potentially be more material when conducted at scale for free-to-access cam services and tube services that rely on high volumes of users but generate relatively low revenue per user, including through advertising views and engagement. In contrast, premium services typically rely on a smaller pool of customers paying for content, with generally higher revenue per user, which makes per-check costs easier to absorb.
- 7.28 The extent to which these cost pressures persist may depend, in part, on how the age assurance market develops over time. Some developments could reduce costs for services, although the extent of their impact remains uncertain at this stage.¹⁸⁶ For example:

¹⁸¹ Free Dating response to our 2025 CfE, pp.2-4; [§<] response to our 2025 CfE, p.8; [§<] response to our 2025 CfE, p.8; Open Rights Group response to our 2025 CfE, p.7; ODDA response to our 2025 CfE, p.2; [§<] response to our 2025 CfE, p.5; Age Check Certification Scheme (ACCS) response to our 2025 CfE, pp. 4-5; BILETA response to our 2025 CfE, p. 9; AVPA response to our 2025 CfE, p. 11.

¹⁸² Free Dating response to our 2025 CfE, p. 4.

¹⁸³ [§<] response to our 2025 CfE, p. 8; ACCS response to our 2025 CfE, pp. 4-5; [§<] response to our 2025 CfE, p.5.

¹⁸⁴ Open Rights Group response to our 2025 CfE, p.7. [§<] response to our 2025 CfE, p.8.

¹⁸⁵ Free Dating response to our 2025 CfE, pp.2-4. Open Rights Group response to our 2025 CfE, p.7; ODDA response to our 2025 CfE, p.2.

¹⁸⁶ We have not assessed the suitability of specific providers or solutions as part of this report. However, Ofcom will continue to engage with age assurance providers to understand the products being offered and maintain our understanding of the market as whole. Regardless of the solution adopted, services are

- Reusable, tokenised, or interoperable age assurance models, including digital ID, may reduce costs where they allow users to rely on an existing age credential and avoid the need to repeat an age check.¹⁸⁷
- Emerging free or lower-cost options in the market may increase competitive pressure in the market and potentially put downward pressure on age assurance costs over time.
- Even where per-check costs could be a concern, commercial arrangements such as fixed-fee or subscription-based models may reduce the extent to which costs increase directly with each additional check, as discussed at paragraph 7.15. This could mitigate cost pressures for some service providers, where those arrangements are available.

Large declines in traffic point to indirect costs associated with service-level age assurance, particularly for pornography services

- 7.29 Age assurance can also generate indirect costs through its effect on user numbers and engagement. Among pornography services, who are required to restrict access to children altogether, its adoption has led to a significant reduction in user traffic. This indicates that age checks deter some users, for example due to reluctance to share personal data, causing them to stop using the service or to reduce the number of sites they visit.¹⁸⁸ Evidence further suggests this has reduced revenue, particularly where business models rely on advertising to large numbers of users.
- 7.30 To assess these effects, we used data from Similarweb to examine changes in traffic to thousands of adult services operating in the UK.¹⁸⁹ Unlike other service types discussed in this report, which may already have had some form of age assurance in place or have not been required to implement age checks for their entire userbase, the deployment of age checks by pornography services offered a clear comparison. This allowed us to better attribute changes in traffic levels to age assurance duties.

Industry-level effects

- 7.31 We examined trends at the industry-level based on data from Similarweb to provide an overview of how overall user activity has changed since the introduction of age assurance.
- 7.32 As shown in Figure 12, the evidence points to an overall contraction of the market, with estimated daily visitors to approximately 21,000 adult services declining by roughly a third since the introduction of age assurance.¹⁹⁰ While our data includes users who activated a

responsible for ensuring it meets our HEAA guidance and is implemented so as to be highly effective in determining whether a user is a child. As discussed in Section 8, we would expect services to conduct thorough due diligence both when selecting age assurance providers and on an ongoing basis when relying on them to deliver age assurance method(s). This includes tracking their accuracy over time and whether they are meeting the latest industry standards.

¹⁸⁷ [X] response to our 2025 CfE, p.8.

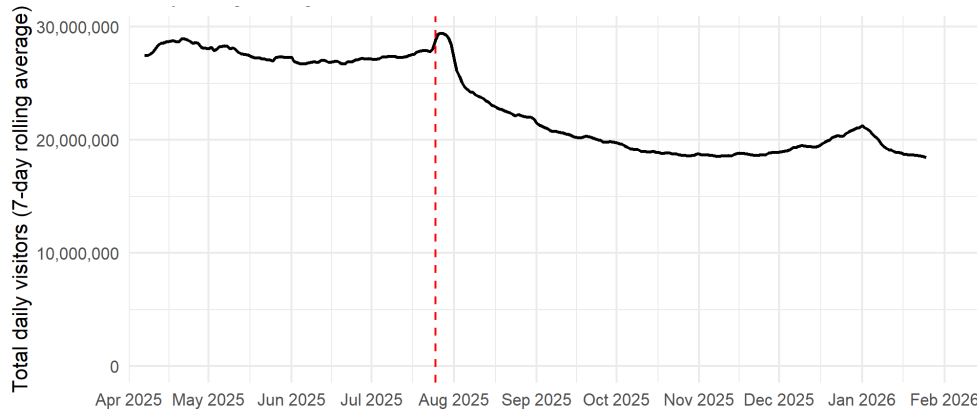
¹⁸⁸ For example, a user may choose to verify their age only on a small number of sites to avoid sharing personal data across several services.

¹⁸⁹ We relied on Similarweb for this analysis given its extensive coverage of adult services operating in the UK, ranging from the largest services to the long tail of smaller sites. This allows for a more comprehensive assessment of the impact of age assurance on the industry compared to other data sources used in this report.

¹⁹⁰ Similarweb defines daily visitors as the average number of individuals who visited a website in one day. Given this metric is not deduplicated across devices, an individual who visits a website from more than one device on a given day can be counted multiple times. Moreover, given that we aggregate daily visitors at the

VPN at the start of a session, it does not capture those who were already connected to a VPN prior to starting their session. This means that some of the decline in Figure 12 may be partly explained by unobserved VPN use.

Figure 12: Total estimated daily visitors to adult services over time



Source: Similarweb. 21,269 adult services analysed, from April 2025 to January 2026. Data extracted on 12 March 2026

- 7.33 The decline may also reflect reduced activity among both child and adult users. These age-specific effects could not be separately identified with the available data. However, [findings from the Lucy Faithfull Foundation](#) show nearly half of surveyed adults (47%) reported reducing the amount of pornography they watched since age assurance duties came into force.¹⁹¹ Such a decline in adult user activity is very likely to translate into lower revenues, for example through fewer ad impressions or premium subscriptions.
- 7.34 This is consistent with evidence from the analysed services. Where revenue losses were reported, these were generally linked to reductions in user activity following the implementation of age assurance.¹⁹² In one case, a service provider reported large declines in user engagement, noting this reduced their ability to generate profit in the UK market.¹⁹³
- 7.35 Taken together, the evidence suggests that age assurance is associated with significant indirect costs. The sharp reduction in estimated traffic points to revenue implications arising from implementation, consistent with evidence provided by a small number of analysed services. Such indirect costs may act as a barrier to deployment. As discussed in Section 4, services with low average traffic levels are less likely to have age checks in place, potentially reflecting a more limited capacity to absorb the decline in traffic and associated revenue effects.
- 7.36 The extent of these effects is likely to depend on a range of service-specific factors, including underlying business models and the monetisation potential of the remaining user base. For example, free-to-access services may experience greater impacts relative to subscription-based platforms, which may be less reliant on advertising revenue and for

industry-level, individuals may also be counted more than once if they visit multiple services in a given day. As such, the metric shown in Figure 12 may overstate the number of distinct users and should be interpreted as indicative of overall activity levels rather than unique individuals.

¹⁹¹ Lucy Faithfull Foundation, January 2026. 'Age verification has changed the way adults are watching porn'.

¹⁹² [3<] 5 analysed service providers' responses to our information notices issued 15 December 2025.

¹⁹³ [3<] response to our information notice issued 15 December 2025.

which user loyalty may also be greater. Similarly, to the extent that the remaining user base is high-value – for example, because they consume content frequently and/or are more likely to pay for premium content – the impact on service revenue may be more limited than implied by traffic levels alone. This is consistent with evidence from the information notice responses suggesting that higher engagement among remaining users meant stable revenue despite declining traffic.¹⁹⁴ However, the overall evidence on these service-specific factors remains limited, meaning it is not possible to draw firm conclusions about the magnitude of these effects or how they may vary across services.

User privacy and data protection

- 7.37 In this section, we consider the steps that services have taken to ensure that their approach to age assurance protects user privacy and complies with data protection legislation. We also consider public concern for user privacy, how these concerns shape user attitudes to age assurance, and whether they reduce user willingness to complete age checks.
- 7.38 Ofcom and the Information Commissioner’s Office (ICO) have been clear that compliance with both the online safety and the data protection regimes is mandatory and should not be considered a trade-off between one and the other. In our HEAA guidance, we set out that service providers who are required to implement age assurance under the Act must also adhere to the requirements of the UK’s data protection regime and should follow a data protection by design approach.¹⁹⁵
- 7.39 We further explained in a [Joint Statement](#) with the ICO that services can process personal data for age assurance, as long as the method is necessary, proportionate to the risks on the service, and complies with data protection legislation. We do not expect services to use age assurance methods that introduce risks to rights and freedoms that outweigh the benefits.
- 7.40 For more information about the main areas of interaction between online safety and data protection laws as they relate to age assurance, see the Joint Statement.¹⁹⁶

Overall, analysed services across sectors demonstrated a strong awareness of privacy and data protection requirements

Data minimisation

- 7.41 Analysed services often cited data minimisation considerations as a driving factor in their choice of which age assurance methods and third-party providers to use. This was consistently referenced across social media, dating, and pornography services.
- 7.42 Many analysed services specifically mentioned not retaining, or minimising the retention, of personal data in their age assurance process.¹⁹⁷ Some of these services specified that personal data and proof-of-age information was immediately deleted, while others stated that no repository of personal data was created.¹⁹⁸ Some of the services that did retain data

¹⁹⁴ [3<] response to our information notice issued 15 December 2025.

¹⁹⁵ Ofcom, 2025. Guidance on highly effective age assurance for Part 3 services, p.7.

¹⁹⁶ Ofcom/ICO, 2026. Age Assurance: A Joint Statement by Ofcom and the Information Commissioner’s Office.

¹⁹⁷ [3<] 21 analysed services’ responses to our information notices issued 15 December 2025.

¹⁹⁸ [3<] 4 analysed services’ responses to our information notices issued 15 December 2025.

reported that retention periods were generally short. For example, one pornography service¹⁹⁹ said that the third-party facial age estimation process retains “facial images” and identity documents for up to one hour (no data is held by the overall third-party provider of age estimation to the service), while its credit card method processes data only for as long as necessary and does not store card data. One social media service said data was generally stored for only 72 hours and for no more than 30 days.²⁰⁰ Another social media service stated that it reduced the retention period for “photographic information” from seven to three days in light of privacy considerations.²⁰¹

- 7.43 Some services described approaches designed to minimise the amount of personal data processed or shared during the age assurance process. Two social media services²⁰² said they use approaches where personal data is only processed on the user’s device, meaning that no facial images or biometric information is ever processed on a remote server. In these cases, minimal decision information is shared with the service, such as a pass/fail outcome, a time stamp and the method used.
- 7.44 Several pornography services also stated that their third-party age assurance providers share only the binary pass/fail outcome in order to preserve the privacy of the user who has completed the age check.²⁰³

Choice of age assurance provider

- 7.45 Services took different views on whether in-house or third-party age assurance solutions better support user privacy. One social media service said it was unable to identify a third-party age assurance provider that was compatible with its “core technical infrastructure and privacy principles”, and that it would not have been able to verify third-party providers’ claims.²⁰⁴ It therefore chose to use proprietary technology, stating that this approach reflected “special adherence to principles of privacy by design and data minimisation, ensuring that no repository of sensitive personal data is created thereby minimizing the risk of malicious actors obtaining such sensitive personal information”.
- 7.46 More commonly, however, services reported choosing third-party age assurance providers to reduce the volume of personal data processed by the service itself.²⁰⁵ Some services also recognised the need to assess providers’ privacy and data protection practices before relying on them. For example, many services across service types stated that a third-party provider’s regard for privacy influenced their procurement decision.²⁰⁶ One service described assessing third-party age assurance providers on privacy, data protection and security as part of its due diligence process,²⁰⁷ while another service said that its third-party review process required privacy, legal and security teams to review data collection and handling processes of third-party providers.²⁰⁸ Two other services referenced contractual

¹⁹⁹ [X] 3 analysed services’ responses to our information notices issued 15 December 2025.

²⁰⁰ [X] response to our information notice issued 15 December 2025.

²⁰¹ [X] response to our information notice issued 15 December 2025.

²⁰² [X] 2 analysed services’ responses to our information notices issued 15 December 2025.

²⁰³ [X] 6 analysed services’ responses to our information notices issued 15 December 2025.

²⁰⁴ [X] response to our information notice issued 15 December 2025.

²⁰⁵ [X] 7 analysed services’ responses to our information notices issued 15 December 2025.

²⁰⁶ [X] 9 analysed services’ responses to our information notices issued 15 December 2025.

²⁰⁷ [X] response to our information notice issued 15 December 2025.

²⁰⁸ [X] response to our information notice issued on 15 December 2025.

requirements or safeguards requiring age assurance providers to adhere to the services' privacy principles.²⁰⁹

- 7.47 Regardless of whether age assurance is delivered in-house or by a third-party provider, regulated services remain responsible under the Act for having a particular regard to the importance of protecting users from a breach of statutory provisions or rule of law concerning privacy.²¹⁰ Services should therefore ensure that their chosen age assurance solution is supported by appropriate data protection safeguards. Where they use third-party providers, this includes seeking robust assurance about the provider's data protection practices, as well as clearly defining the roles and responsibilities of their third-party provider in terms of who is the data controller. Please see Section 8 where we detail the practical improvements that services should make, including conducting due diligence on their age assurance vendor.

Choice of age assurance method

- 7.48 In some cases, regard for user privacy influenced the choice of age assurance method and the way services layered different methods. Five services specifically mentioned conducting data protection impact assessments for parts of their age assurance processes, to support the assessment of proportionality and necessity of age assurance methods.²¹¹
- 7.49 Most social media services using age inference said they assessed the relative friction, effectiveness and privacy impact of different age assurance approaches and chose methods they considered proportionate to the risk.²¹² They said they did not choose methods requiring official identity documents as their primary approach because this would have required the large-scale collection of personal data from younger users, making it more intrusive than necessary. Instead, they chose an age inference approach which, according to these services, allowed them to meet the objective of protecting children while minimising the amount of additional data needing to be collected.
- 7.50 The use of age inference models raises privacy and data protection questions. The ICO are clear that any deployment of age assurance technology, including age inference or profiling, must consider user privacy and comply with data protection law.²¹³ In relation to the use of profiling as part of an age assurance system, the ICO is clear that profiling for age assurance does not function as an age-gating measure (for example, age verification or age estimation techniques which can be used to prevent access to a service or functionality at the point of entry). In reviewing current industry use of profiling for age assurance, the ICO considers that it is not currently an effective method for preventing underage users from accessing a service that is unsuitable for them.²¹⁴ The ICO provides further information about the risks associated with what they call "profiling" for age assurance [here](#).²¹⁵

²⁰⁹ [3] 2 analysed services' responses to our information notices issued on 15 December 2025.

²¹⁰ Section 22(3) of the Act.

²¹¹ [3] 6 analysed services' responses to our information notices issued on 15 December 2025.

²¹² [3] 3 analysed services' responses to our information notices issued on 15 December 2025.

²¹³ Information Commissioner's Office (ICO), accessed on 8 May 2026. Annex: What we've learned about profiling for age assurance.

²¹⁴ ICO, accessed on 11 June 2026. [Children's Code Strategy Progress Update – December 2025](#), Annex: What we've learned about [profiling for age assurance].

²¹⁵ ICO, accessed on 8 May 2026. [Profiling](#); ICO, accessed on 8 May 2026. [Profiling tools for online safety](#).

- 7.51 Other services also described choosing methods that limited extensive data collection. One social media service stated it chose methods that balance effectiveness with low privacy intrusion, including by using existing signals and information, such as account creation date rather than collecting additional data.²¹⁶ One service provider said it chose facial age estimation that could be integrated into the account creation process partly because it did not require “the routine collection or storage of identity documents for all users”.²¹⁷ It explained that photo ID matching is reserved for specific circumstances, such as where a user is deemed to potentially be underage or appeals an age check outcome.

Informing and involving users

- 7.52 A few services described the steps taken to inform users about their age assurance processes. One social media service described providing privacy information in an accessible format with the audience of teenagers in mind.²¹⁸
- 7.53 One service provider explained that it provides information to users about the use of their images through in-app notices and supporting materials, in order to help users understand how their data is used.²¹⁹ One pornography service noted that it outlines its disclosures around data collection and consent for users in its privacy policy.²²⁰
- 7.54 In the subsequent section we explore in more detail public concerns for user privacy in relation to age checks, which suggests that more could be done to inform users about how their age assurance process protects users’ data.

Public concern about data protection and user privacy persists

- 7.55 Adults continue to express strong concerns that completing an age check might compromise their user privacy or personal data. We saw evidence of increased awareness of personal data, privacy, and security issues in Ofcom’s annual Adults’ Media Lives study.²²¹ This increased awareness was partly attributed to high-profile cyber-attacks. When prompted with information on the Act and age assurance specifically, almost all participants were supportive in principle of stricter age checks where relevant. However many had concerns about the security of data being collected for this purpose, and several said they had heard that systems have been hacked. One participant said “there’s no way I’m sticking my passport details in a random website”.²²²
- 7.56 Consistent with this, responses to our 2025 CfE indicated that data protection and privacy were a key concern in the context of age assurance, with it being the most commonly occurring theme. In general, stakeholders commented that users remain cautious about sharing ID documents or biometric information, fear data breaches, and in some instances therefore try to avoid undergoing age assurance.²²³

²¹⁶ [X] response to our information notice issued 15 December 2025.

²¹⁷ [X] 3 analysed services’ responses to our information notices issued 15 December 2025.

²¹⁸ [X] response to our information notice issued 15 December 2025.

²¹⁹ [X] 3 analysed services’ responses to our information notices issued 15 December 2025.

²²⁰ [X] response to our information notice issued 15 December 2025.

²²¹ Ofcom, 2026. Adults’ Media Lives Report.

²²² Ofcom, 2026. Adults’ Media Lives Report.

²²³ Internet Matters response to our 2025 CfE, pp.4-5; Free Dating response to our 2025 CfE pp.2-3; ODDA response to our 2025 CfE, p.3; Ukie response to our 2025 CfE, p.7; AVPA response to our 2025 CfE, pp.5-6.

- 7.57 Several stakeholders cited incidents where privacy failures damaged public trust in age assurance systems. ODDA said recent high-profile data breaches have increased users' privacy concerns, with smaller platforms seeing higher drop-off rates due to lower user trust.²²⁴ AVPA described a well-publicised breach involving a third-party customer-service provider handling age assurance-related data. It said that the system was not designed for sensitive data, and better data minimisation and transparency would have reduced impact.²²⁵
- 7.58 Free Dating²²⁶ specifically referenced the incident involving Discord and the third-party service provider 5CA, where approximately 70,000 users may have had government ID photos (which the service provider used to review age-related appeals) exposed.²²⁷ These incidents illustrate the importance of designing and implementing age assurance processes in line with data protection obligations to prevent and mitigate data breaches and thus support the effectiveness of the age assurance process.
- 7.59 Internet Matters cited [its research](#) from April 2025 that found privacy is the top concern for parents (43%), followed by uncertainty about how data is used (35%).²²⁸ AVPA said that users sometimes distrust third-party age assurance providers when redirected from familiar services to unfamiliar ones.²²⁹
- 7.60 Our 'Proving Age' survey also found strong privacy and personal data protection concerns among users. Among the lapsed users of pornography services who said they did not plan to access pornographic content in future due to concerns about proving their age, 94% identified at least one concern related to personal data. In this group, 76% selected not wanting to share their personal information when accessing websites with pornographic content, 75% were worried their personal information would not be protected if they proved their age, and 71% said they did not trust the third-party providers that companies used to verify age.²³⁰
- 7.61 Among active users of online pornography services in the Proving Age survey, personal data concerns underpinned non-completion among both those who chose not to prove their age and those who have ways of bypassing age checks (96% for both). In addition to this, around half (52%) of active users of online pornography say they "always" use "private browsing mode" to access pornographic content online and 78% said that they use private browsing mode to do this at least some of the time, demonstrating that privacy is an active consideration among this cohort.²³¹
- 7.62 These findings suggest that privacy concerns may affect whether users are willing to complete age assurance. Greater clarity, transparency, and accessibility in user-facing explanations about the data that services require and how it is processed may strengthen

²²⁴ ODDA response to our 2025 CFE, p.3.

²²⁵ AVPA response to our 2025 CFE, pp.4-5.

²²⁶ Free Dating response to our 2025 CFE, pp.2-3.

²²⁷ Discord Press Release, October 2025. '[Update on security incident involving third-party customer service](#)' [Accessed 23 April 2026].

²²⁸ Internet Matters response to our 2025 CfE, pp.4-5; Internet Matters, 2025. 'Age assurance and online safety: what parents and children have to say'. Accessed on 11 May 2026.

²²⁹ AVPA response to our 2025 CfE, pp.5-6.

²³⁰ Ofcom, 2026. Proving Age to Access Online Pornography Survey.

²³¹ Ofcom, 2026. Proving Age to Access Online Pornography Survey.

user trust in age assurance processes. This is highlighted as a practical area of improvement in Section 8.

Bypassing or circumventing age checks

- 7.63 In this section, we consider the extent to which users may be bypassing or circumventing age assurance, and whether this may prevent or hinder the effective use of age assurance. We assess evidence about the use of VPNs as well as other techniques, such as providing false or fabricated information and attempts to manipulate the age check itself.
- 7.64 Our evidence suggests that VPN use has increased among UK users, but does not currently show that this increase is due to children motivated by a desire to bypass age checks on online services. Evidence on circumvention techniques is limited but indicates that robust configuration and monitoring of age assurance processes is important to mitigate known and emerging risks.
- 7.65 Evidence on users avoiding age checks by migrating to services that do not have age assurance in place is explored in Section 4 due to the specific role this plays in the pornography sector.

Evidence suggests that some children use VPNs for a variety of activities online

- 7.66 VPNs are used across the UK for a variety of reasons including privacy and security assurances.²³² However, because VPNs allow internet users to change their virtual location and internet protocol (IP) address to another country, they can also be used to bypass protections of the Act, including age assurance. This has featured prominently in public debate about the capability of age checks to protect children online.
- 7.67 Our research shows a significant increase in general VPN use immediately following the implementation of age assurance in July 2025. Our latest analysis shows a sustained higher level of VPN use since the initial spike, with the estimated number of daily UK VPN users being 2.2 million compared with 1.2 million daily users prior to 25 July 2025.²³³ It is not possible, using this dataset, to establish the proportion of this increase that is driven by children, however we explore the available evidence that demonstrates children's use of VPNs as well as the activities they use them for.
- 7.68 Our research on children's use of VPNs, conducted in March 2026 with GB children aged 11 to 17, found a quarter of children had used a VPN in the previous six months. This proportion increased with age, to 31% among 16 to 17-year-olds compared to 16% among 11 to 12-year-olds.²³⁴

²³² Paragraph 7.67 sets out the estimated number of daily UK VPN users.

²³³ Similarweb estimated daily active users for VPN mobile apps, based on aggregated app usage data across iOS and Android devices, data extracted on 7 May 2026. This data reflects our latest view of VPN usage based on Similarweb and is consistent with other data used in this report. This updates Ofcom's previous view which was based on a different data supplier that showed a slightly lower number of daily VPN users and a drop off in the total number of VPN users after an initial spike. Note that it is not possible to determine the specific purpose or reason behind the VPN use with this data.

²³⁴ Ofcom, 2026. Children's use of VPNs.

- 7.69 Our study conducted with parents in October 2025 indicated some increase in children’s use of VPNs in the three months immediately following age assurance implementation. When asked about any changes in their child’s online experiences in the three months prior to fieldwork, 4% of parents said that their child had started to use a VPN for the first time, while 3% reported their child had used a VPN more frequently.²³⁵
- 7.70 Research conducted in February 2026 found that three quarters (77%) of 16 to 17 year olds say they have ever used a VPN, with this rising to nearly nine in ten (87%) among those who are active users of online pornography.²³⁶ This is an increase on the previous wave of research (78%) conducted in September 2025.
- 7.71 In responses to our 2025 CfE, stakeholders likewise reported an increase in VPN adoption following the children’s safety duties coming into force, with three stakeholders²³⁷ mentioning [Childnet research](#) from December 2025, that reported 21% of children aged 8 to 17 having used a VPN.²³⁸
- 7.72 In terms of what children use VPNs for, 5% of children in this study said they had used a VPN in the past six months to either access content meant for people older than them, or to access features and functions with age restrictions.²³⁹ In a separate study, a similar proportion (5%) told us they had circumvented highly effective age restrictions in the past 12 months.²⁴⁰ Both studies may understate the proportion of children circumventing these restrictions due to response bias, such as a reluctance to disclose this behaviour to a researcher.
- 7.73 The Childnet research mentioned in response to our 2025 CfE showed that the most common reasons given for using VPNs were to stay safe online and protect privacy, selected by 38% of respondents using a VPN. Internet Matters said there is emerging evidence that a small number of children are using VPNs specifically to bypass age checks, in some cases with parents actively helping them.²⁴¹ Internet Matter’s May 2026 research found that 7% of children who said they had bypassed age checks had done so via VPN.²⁴²
- 7.74 Taken together, the available evidence suggests that VPN use has increased, and there is evidence that some children use VPNs.

There is evidence to suggest users circumvent age checks, but the extent and impact is uncertain

- 7.75 Some users may circumvent age checks by using techniques that undermine the legitimacy of the age check itself. These include biometric presentation attacks or completing an age check by providing false or fabricated information. AVPA reported instances of these behaviours, including the use of fake driving licences generated online or the use of avatars

²³⁵ Ofcom, 2026. Parents’ Perceptions of Protection of Children Measure Study.

²³⁶ Ofcom, 2026. Proving Age to Access Online Pornography.

²³⁷ [3<] response to our 2025 CfE, p.6; UK Safer Internet Centre response to our 2025 CfE, p.3; [3<] response to our 2025 CfE, p.9.

²³⁸ Childnet, December 2025. Young people’s use of VPNs.

²³⁹ Ofcom, 2026. Children’s use of VPNs.

²⁴⁰ Ofcom, 2026. Children and parents: media use and attitudes.

²⁴¹ Internet Matters response to our 2025 CfE, pp.3, 5.

²⁴² Internet Matters, 2026. [The Online Safety Act: Are children safer online?](#) p.16.

from computer games.²⁴³ However, AVPA noted that such attacks are typically only successful where services have disabled or weakened key safeguards designed to prevent such attacks. This indicates that these risks can be mitigated through robust configuration of age assurance processes.

- 7.76 In our Children and Parents Media Use and Attitudes Report, a minority (16%) of children aged 13 to 17 told us that they know how to circumvent highly effective age gates, but as noted above, fewer (5%) told us that they had done so in the past 12 months.²⁴⁴ One of the ways children may circumvent age assurance is by using accounts belonging to adults, or by relying on an adult to complete an age check on their behalf. For example, a parent or older sibling may complete an age check so that a child can access specific content, or they may allow their personal details to be used, such as an ID document or credit card details. In some cases, children may have an account that is shared with an adult who has completed an age check and therefore the child has unrestricted access to a service.
- 7.77 Our Adults' Media Lives study found that adults were dubious about how effective age checks would be in practice, and highlighted the possibility of children circumventing age checks. One participant said "they'll find a way around it. I mean, no doubt, teenagers will find a way around it", while another said that "they'll just get someone else to log in on their behalf". Another participant highlighted how easy it could be for a child to have their parent complete an age check for them by asking them to take a photo.²⁴⁵
- 7.78 Users may also disguise, obscure, or manipulate signals that the age assurance method relies upon through presentation attacks. This might include face spoofing in liveness checks, for example using filters, masks, or printed images to interfere with facial age estimation. BILETA raised concerns about the accuracy of facial age estimation and whether these systems can be "defeated" by user behaviour, giving the example that the facial age estimation systems used by Reddit and Discord could reportedly be tricked with images of an adult character from a video game.²⁴⁶
- 7.79 AVPA also highlighted that social media was a key factor in amplifying these circumvention tactics, as users posted about it, enabling copycat attacks. In their 'Lessons learned from AV day' report, AVPA stated that adversarial attacks and emerging threats were 'low volume', but they demonstrate that new attack vectors can arise quickly.
- 7.80 We have reason to believe that some determined children are finding ways to bypass or circumvent age checks using a small range of techniques. However, at this early stage we do not have reliable evidence with large enough sample sizes to determine the scale of

²⁴³ AVPA response to our 2025 CfE, p.3.

²⁴⁴ Ofcom, 2026. Children and Parents: Media Use and Attitudes Report. 16% of participants said they knew 'how to around age checks (e.g. providing credit card details, sharing a photo ID, or scanning your face) that are there to stop you visiting certain sites or apps or accessing certain content'. 5% of participants said they had. **Note:** data may understate the proportion of children circumventing restrictions due to response bias, such as a reluctance to disclose this behaviour to a researcher.

²⁴⁵ Fieldwork took place between 6 October 2025 and 31 October 2025, and as such reflects the views of participants at this time. There was confusion around highly effective age assurance and other restrictions (such as using betting websites), which could have an impact on respondents' opinions on how effective it could be to bypass. Ofcom, 2026. Adults' Media Lives Report.

²⁴⁶ BILETA response to our 2025 CfE, p.4 (citing: Tom Warren, '[Reddit and Discord's UK age verification can be defeated by Death Stranding's photo mode](#)' (The Verge 28 June 2025). [Accessed 18 Nov 2025]).

circumvention by children. Nevertheless, these behaviours and their associated risks underline the importance of services configuring and maintaining their age assurance processes in ways that ensure robustness and reduce the risk of circumvention by children. This includes making sure that relevant safeguards are in place and working effectively, such as liveness checks and document authenticity checks, and monitoring emerging circumvention techniques as appropriate.

8. Summary of issues and suggested improvements

- 8.1 Throughout this report we have highlighted areas where we observed that analysed services' age assurance implementation has fallen short of our expectations and is not in line with our HEAA guidance.
- 8.2 To assist Part 3 and Part 5 services in making the expected improvements to their age assurance process, we have set out the issues and suggested improvements in the below table. In general, these issues and improvements are not specific to certain service types and are therefore applicable across service types.
- 8.3 Services should consult our HEAA guidance for further context when reviewing their existing age assurance process against these areas for improvement. Services should implement the necessary changes as a matter of urgency.

Figure A1: Summary of issues and improvements in age assurance processes from year 1

Observation	Improvement
Follow our HEAA guidance in full	
Some services using facial age estimation have not implemented a challenge age.	To improve robustness, services using facial age estimation should use a challenge age approach to reduce the likelihood of misclassification of children as adults, set according to the technical accuracy of the method. If this is not technically feasible then we would expect services to demonstrate an equally effective mechanism that reduces the likelihood of false positives. We expect services to be able to demonstrate how the chosen approach reduces the likelihood of children being exposed to harmful content.
Some services that use facial age estimation or photo ID matching did not have liveness detection in place	To improve robustness, services using facial age estimation or photo ID matching should put liveness detection in place . This reduces the risk of children using still images of adults or prerecorded videos to circumvent these methods.

Observation	Improvement
Many services rely on a one-time age check and do not require users to repeat age checks.	Services should consider repeating age checks and/or introducing targeted and proportionate anti-circumvention measures after an initial age gate to increase the robustness of their process. This includes assessing whether repeat age checks are needed to secure the robustness of their solution, and if so, how often is it appropriate to repeat an age check, and if there are certain triggers that increase the need for repeating age checks (such as suspicious behaviour or new log ins).²⁴⁷
We observed variation in the number of age assurance methods that services offer users, with some services only offering one method.	Services should consider offering a variety of age assurance methods to improve the accessibility of their age assurance process. This may help to assist users who may be unable to use certain kinds of age assurance or may find it more difficult.
Many services with age assurance in place have not fully implemented an appeals process to restore a user's access where they have incorrectly had it restricted.	To increase fairness and in line with measures PCU D11 and PCU D12 in the Protection of Children Codes, services should offer users an age assessment appeals process to take appropriate and prompt action. Services should track and monitor appeals numbers and the proportion of appeals upheld. Where services have high proportions of appeals upheld, they should investigate the reasons for these appeals (including whether the issue is with the appeal process itself or with the initial age check). Services should seek to identify and remedy any common reasons for failure.
Conduct regular due diligence on any age assurance vendor you employ and your age assurance process	
Several services do not appear to be regularly evaluating their age assurance process against appropriate metrics to understand if the process is highly effective.	Services should assess what information they need to collect and evaluate to know how effective the process is. Suggested metrics are outlined in the technical glossary of our HEAA guidance. Services should measure and monitor performance using appropriate metrics, while meeting their data protection obligations. We also advise services to track and monitor the proportion of users that their age assurance process determines as over 18 (or over the respective challenge age). Where services identify this as being particularly low or high, services should consider whether they implemented their age assurance process in line with our HEAA guidance, including the technical accuracy criterion.

²⁴⁷ Services must also ensure they are meeting their data protection obligations, including regarding necessity, proportionality and data minimisation.

Observation	Improvement
Services who rely on third party vendors may not be doing their due diligence sufficiently to check the solution is highly effective.	Where services are relying on third-party solutions, they should conduct regular and thorough due diligence on their age assurance vendors. This includes checking the appropriate metrics are measured (as outlined above) and ensuring no changes to important configuration settings that may undermine the effectiveness of the third-party solution. It is the service's responsibility to ensure that their age assurance process is implemented in such a way that it is highly effective at correctly determining whether or not a particular user is a child.
Comply with your privacy and data protection obligations	
User privacy and data protection remains a priority concern among the public in relation to age checks, and in some cases may have driven attempts to bypass or circumvent age assurance.	When implementing age assurance, services should consult the relevant ICO guidance to ensure their age assurance process fulfils data protection obligations. As part of this, services must implement appropriate measures to provide clear, understandable and easily accessible information to users about how their data is processed, used, and deleted, particularly where the information is addressed specifically to children. This could include providing information in plain English or multiple formats, including child friendly formats. Greater transparency and accessibility in these areas would support user understanding and confidence in how personal data is handled within their age assurance processes, and may encourage user trust and engagement with age assurance. The Ofcom-ICO Joint Statement on Age Assurance is a helpful resource for services to check they are complying with both online safety and data protection legislation.

A1. Methodology

Ofcom research sources

Children's Online Safety Tracker (COST)

- A1.1 The [Children's Online Safety Tracker \(COST\)](#) is designed to monitor the online experiences of UK children aged 8 to 17, including their awareness and use of online safety tools, and their recalled exposure to harmful content online.

COST Methodology outline

- A1.2 COST is conducted on an online panel, where children are recruited via their parents. At the time of publication, two waves of the study have been analysed.

- **Wave 1:** March 2025 to April 2025, prior to the children's safety duties coming into force on 25 July
- **Wave 2:** November 2025 to December 2025, approximately four months after the children's safety duties came into force.

- A1.3 The survey uses a **modular design**, with children completing either:

- **Module 1:** Use of online safety tools, or
- **Module 2:** Exposure to harmful content online.²⁴⁸

Wave 1

- A1.4 The total sample achieved at Wave 1 was **3,142 children aged 8 to 17**. Of these, **1,746 children** completed Module 1 (ages 8 to 17) and **1,396** completed Module 2 (ages 11 to 17).

Wave 2

- A1.5 The total sample achieved at Wave 2 for the online panel was **3,387 children aged 8 to 17**. Of these, **1,735** children completed Module 1 (ages 8 to 17) and **1,625** completed Module 2 (ages 11 to 17).

Timeframe

- A1.6 All survey responses are based on children's recall of experiences during the **four weeks prior to survey completion**.

Recall

- A1.7 Responses reflect respondents' own recall and judgement. The harms codes used in this research were cognitively tested with children to ensure they were broadly understood as intended. However, as with any self-reported measure, there may be some degree of individual interpretation in how children classify and recall their experiences. Despite this, the results are considered valid and, crucially, any such interpretation is expected to be consistent across waves. This means that trends over time remain robust and provide a reliable indication of changes in children's experiences.

²⁴⁸ This module was delivered via an online panel and restricted to respondents aged 11 to 17 for safeguarding reasons, given that the questions related to harmful topics.

Changes at Wave 2

- A1.8 At Wave 2, changes were made to the COST survey. These included:
- Expansion of harmful content included in Wave 2 to include questions about children's recalled exposure with **non-designated content (NDC)**. Trend analysis within this report is therefore limited to exposure of PPC and PC only. Data on children's exposure to NDC is available online.
 - Revisions were made to the list of services included. At Wave 2, "online games" was replaced with individual codes for gaming services such as Roblox, Call of Duty, and Minecraft.

Children's Passive Online Measurement (CPOM)

- A1.9 [Children's Passive Online Measurement \(CPOM\)](#) measured the use of websites and apps across smartphones, tablets, and computers by a UK-representative sample of children aged 8 to 14. The study captured which services were visited and how long children spent on the service, based on passive monitoring of the devices rather than survey recall.
- A1.10 In Phase Two of the study, we collected data from a nationally representative sample of 701 children, passively measuring their visits of websites and apps across the smartphones, tablets, and computers that they use to go online. The children had passive monitoring software installed on the device(s) they used to go online, with data collected anonymously. Each child was monitored for **28 consecutive days**, with fieldwork conducted on a rolling basis between **9 October 2025 and 7 March 2026**. Findings therefore reflect usage patterns during this period and are not necessarily representative of children's internet use across a full calendar year.
- A1.11 All figures provided are estimates that will have some margin of error.

Adults' Media Lives

- A1.12 [Adults' Media Lives](#) is a longitudinal qualitative study conducted with a panel of 20 people selected to reflect a broad cross-section of the UK population in terms of age, gender, location, ethnicity, and socio-economic background. The study has been running since 2005. All participants from the previous wave (wave 20) took part again this year (wave 21), and more than half of the sample have participated for over 15 years.
- A1.13 Adults' Media Lives provides rich contextual insight into media trends and examines how technology and media fit into individual lives. Adults' Media Lives findings should be read as illustrative and illuminating, rather than as fully representative of the population.
- A1.14 Fieldwork consisted of in-depth filmed interviews conducted between 6 October 2025 and 31 October 2025 by Mark Ellis, Laurie Dempsey, and Tony Harbron of The Knowledge Agency. Seventeen interviews took place face-to-face and three were conducted online.
- A1.15 Certain subjects are tracked each year, including:
- acquisition of new media hardware (such as smart TVs, smartphones, smart speakers, wearable technology) and services (such as super-fast broadband, streaming services);
 - development of media literacy skills, confidence in the use of digital media, and adoption of new online activities (such as the use of AI tools/applications);

- the role of the internet in daily life (such as education, work, shopping, banking, interacting with government and other institutions);
- viewing and listening behaviour and other content consumption;
- sources of news and information;
- trust in content and media providers across different media platforms; and
- concerns about personal data, privacy, and security.

A1.16 However, the research model is flexible enough to explore specific new areas of interest each year (for example, attitudes to the introduction of highly effective age assurance under the Online Safety Act 2023 (the Act)).

Children's experiences of being asked to verify their age

- A1.17 The [Children's experiences of being asked to verify their age tracker](#) was a quantitative online study conducted across four waves, each taking place every two months. It was designed to track children's exposure to age-assurance requests between July 2025 and January 2026 and to monitor changes from the pre-implementation to post-implementation of age-assurance measures, particularly the prevalence of age assurance methods that could be classified as highly effective age assurance across different online services.
- A1.18 Each wave surveyed a sample of 1,000 GB children aged 8 to 17. Wave 1 took place between **17 July 2025 and 24 July 2025 (prior to the children's safety duties coming into force on 25 July)**. All other waves ran post implementation of the children's safety duties. Wave 2 ran between **17 September 2025 and 23 September 2025**; Wave 3 between **17 November 2025 and 30 November 2025**; and Wave 4 between **19 January 2026 and 29 January 2026**.
- A1.19 The questions in this tracker were put to GB children aged 8 to 17 who had their own profile on at least one of the social media sites of apps about which we asked.²⁴⁹ Therefore, the findings relate to GB child social media users aged 8 to 17 rather than UK children aged 8 to 17 as a whole.

Children's use of virtual private networks (VPNs) survey

- A1.20 The [Children's use of VPNs](#) research is a **quantitative online study** conducted among **GB children aged 11 to 17**.
- A1.21 The study examined children's use of VPNs by asking whether they had taken part in a range of online activities in the past six months that could involve VPN use, and then which method they used to carry out this activity (VPN being one of the options provided). The survey also measured general frequency of VPN use which was not activity specific.
- A1.22 Fieldwork was conducted between **12 and 26 March 2026**. The total sample size was **2,167 children aged 11 to 17** and the data was representative of GB children aged 11 to 17.

²⁴⁹ The sites or apps about which we asked in the Age Assurance mini wave tracker were: Facebook, YouTube (not including YouTube Kids), Snapchat, Instagram, TikTok, X/Twitter, Discord, Pinterest, Twitch, Reddit, Roblox, and Other (please specify).

Parents' Perceptions of Protection of Children Measures Study

- A1.23 This research is a [quantitative online study](#) conducted among UK parents.
- A1.24 The study examined parents' awareness of protection of children measures in general and of a range of specific children's online safety rules, including age assurance checks. The study also examined parents' attitudes to protection of children measures; in particular whether they felt that these measures either already had or would in the future make their children safer when online. The second wave also looked at whether parents had noticed any changes to their children's experiences online since the children's safety duties coming into force on 25 July 2025.
- A1.25 Fieldwork for Wave 1 of this study was conducted between **3 July 2025 and 9 July 2025**. The total sample size for Wave 1 was **1,400 adults who were parents of children 17 and under**.
- A1.26 Fieldwork for Wave 2 of this study was conducted between **22 October 2025 and 27 October 2025**. The total sample size for Wave 2 was **1,521 adults who were parents of children 17 and under**.
- A1.27 For both waves, the data was weighted to be representative of UK adults (aged 18 and over).

Ipsos iris audience measurement service

- A1.28 Launched in early 2021, Ipsos iris is the UKOM (UK Online Measurement)-endorsed currency for the measurement of audiences of online content of UK people aged 15 and over who use the internet at least once a month.
- A1.29 Ipsos iris uses a hybrid methodology with several data sources, including:
- A passive single-source panel of over 10,000 people aged 15 and over who use the internet. Panellists install passive tracking software onto personally used digital devices and in some instances those who also use their device for work (smartphones, computers, and tablets) which access the internet, with data collected continuously. The panel is recruited to be representative of the internet population demographically, geographically and by device type use.
 - Census measurement of publisher websites and apps to collect visit measures for time spent and page views at a total level.
- A1.30 Reporting on daily and monthly data, all sources are fused together to create a synthetic dataset with more than one million records to represent the UK online infrastructure of websites and apps. These can be analysed and reported at many demographic and geographic levels. As this is a synthetic dataset, it is not possible to provide confidence intervals/ranges for extrapolated population estimates. However, all extrapolated population figures provided are estimates that will have some margin of error.
- A1.31 This report draws on data from a sample of roughly 128 15 to 17-year-olds. Data from this cohort is reported [within our CPOM report](#).

Proving age to Access Online Pornography Survey

- A1.32 The [Proving age to Access Online Pornography](#) survey was commissioned to enhance our understanding of online pornography users' attitudes toward age checks on adult websites.

It explored the impact of highly effective age assurance implementation on user trust and behaviours, including the use of VPNs to access adult content.

A1.33 The research specifically aimed to explore:

- how people access online pornographic content, including their use of VPNs, search engines, private browsing, and clearing browsing history, when accessing adult content;
- online pornography users' previous experiences with age checks online;
- online pornography users' attitudes toward the use of age checks online; and
- barriers that prevent them completing age verification.

A1.34 This study looked at the behaviours of people aged 16 and over who self-reported having previously accessed pornographic content online – both those that had done so before and planned to again (“active users”) and those who had done so before but did not plan to again (“lapsed users”).

A1.35 For Wave 1 of the study, a total of 5,580 interviews were conducted, and fieldwork took place between 5 September 2025 and 23 September 2025.

A1.36 For Wave 2 of the study, a total of 5,591 interviews were conducted, and fieldwork took place between 2 February 2026 and 24 February 2026.

A1.37 The samples in both waves of the study were not nationally representative. Instead, quotas were set on age and gender to align with the demographic profile of X-rated adult site/app users. This resulted in more male than female respondents in each of the two samples (73% male and 27% female in Wave 1 and 75% male and 25% female in Wave 2).

Children and Parents: Annual Media Use and Attitudes Report (CaP)

A1.38 The [Children and Parents: Media use and Attitudes report](#) is an annual longitudinal study that provides evidence on media access, use, attitudes and understanding among children aged 6 months to 17-year-old. The survey also captures parents' views on their children's media use, including how parents monitor and manage media use among children in this age group.

A1.39 The survey asks questions of children aged 8 to 17 directly, with parents answering on behalf of younger children (6 months to 7 years). It uses a mixed-mode approach, combining online and face-to-face interviews to ensure robust coverage across age groups and demographics.

A1.40 A total of 5,008 interviews were conducted for the 2025/6 tracker, including 1,582 interviews with parents of children aged 6 months to 17-year-old and 3,426 interviews with children themselves aged 8 to 17. Fieldwork was conducted between November 2025 and February 2026.

A1.41 Please note that in 2025, we conducted a full review of the survey which resulted in methodological and questionnaire changes. This included streamlining the research into one overarching survey, introducing face-to-face interviews, expanding the sample as well as adapting the questionnaire. This means that this year, our trends over time are indicative rather than absolute as some year-on-year changes are likely to reflect the changes in methodology and question design rather than changes in behaviour alone, although genuine shifts in children's media use may be present.

- A1.42 For the purposes of this report, the data focuses only on children aged 8 to 17.
- A1.43 Further information about CaP, including detail on methodological and questionnaire changes, and access to previous reports, can be accessed on our website at the link above.

Key limitations to the report

- A1.44 There are several important limitations to recognise when considering the findings of this report.
- A1.45 In summary, the main research limitations were:
- The research sources we draw on are not intended to establish causal inference between the introduction of age assurance and changes to children's online experiences.
 - Research primarily represents a point-in-time analysis, but we know that services' implementation of age assurance evolves over time. To mitigate this, we have done four waves of the age assurance mini tracker and two of the proving age survey. Furthermore, both COST and CPOM are on-going trackers so we are building up an ongoing picture of what is happening with regard to children's experience of age assurance, and this will continue (through the trackers) after this report.
 - Methodological complexity, such as research design difficulties in researching the impact of age assurance and research sources that rely on children's recalled exposure to harm. However, the addition of CPOM is valuable here as this is passive monitoring rather than recalled exposure.
 - Incomplete sample of providers: We have constrained the sample of providers who we sent information notices, to a small subset for proportionality reasons. While this is not representative of all services in scope of age assurance, it does provide meaningful insight into how services across the three service types are implementing age assurance.

A2. Detailed analysis of services' regard for highly effective age assurance criteria

- A2.1 This section examines how services have had regard to the criteria and principles set out in our HEAA guidance. We highlight the steps that services have taken to improve effectiveness.

Technical accuracy

- A2.2 In our HEAA guidance, we defined technical accuracy as the degree to which an age assurance method can correctly determine the age of a user under test lab conditions.²⁵⁰
- A2.3 In general, responses to the information notices indicated that services had considered how to ensure their process was technically accurate, but evidence of how this was achieved in practice varied. In this section we set out an overview of how services had regard to technical accuracy, via using metrics and testing, challenge age approaches, and ongoing monitoring and reviews.

Metrics and testing

- A2.4 In general, services stated that they considered relevant performance metrics when assessing the technical accuracy of age assurance methods. The metrics referenced included precision, recall or true positive rates, false positive and false negative rates, and mean absolute error.
- A2.5 Where services relied on third-party age assurance providers, they commonly stated that testing was carried out by the third-party²⁵¹ and that they considered testing and/or the specific performance metrics in use as a factor when determining which provider to use.²⁵²
- A2.6 Several services stated that their chosen age assurance providers had been subject to independent testing or certification, including through schemes such as the UK Age Check Certification Scheme, National Institute of Standards and Technology testing, International Organisation for Standardisation (ISO)-based certifications and Technology Readiness Levels.²⁵³

Challenge age approaches

- A2.7 Responses to the information notices indicated that just under two-thirds of services using facial age estimation had applied a challenge age.²⁵⁴ Among those that applied a challenge

²⁵⁰ Technical accuracy is covered in paragraph 4.29- 4.44 of our Part 5 HEAA guidance; paragraph 4.8 – 4.21 of the Part 3 HEAA guidance.

²⁵¹ [3<] 13 analysed services' responses to our information notices issued 15 December 2025.

²⁵² [3<] 12 analysed services' responses to our information notices issued 15 December 2025.

²⁵³ [3<] 8 analysed services' responses to our information notices issued 15 December 2025.

²⁵⁴ [3<] 19 analysed services' responses to our information notices issued 15 December 2025.

age, the most commonly occurring value was 21, with reported values ranging from 20 to 25.

- A2.8 Two pornography services each use several age assurance providers for facial age estimation solutions, which do not apply a challenge age as described in our HEAA guidance. One of these services described that particular facial age estimation solution as being a “no threshold model”²⁵⁵ while the other said that its solution “does not have any predefined challenge age thresholds” and instead applies “a multi-layer AI model to determine age.”²⁵⁶ It said this “is configured to return a binary yes/no response based on the specific age of interest legally required under each applicable region in each jurisdiction.” We urge services to implement a challenge age to improve the overall effectiveness of the age assurance process. It is the services’ responsibility to ensure that the solution they use is configured appropriately so that risks around the age boundary are systematically mitigated. Where it is not technically feasible then we would expect services to demonstrate an alternative mechanism that reduces the likelihood of false positives.
- A2.9 The absence of a challenge age or equivalent alternative mechanism when using a facial age estimation solution is concerning, because it is necessary to prevent or minimise borderline cases where the age estimation method incorrectly assesses a user as being an adult when they are a child. We are engaging with the relevant services on this matter.

Ongoing monitoring and periodic reviews

- A2.10 In relation to ongoing monitoring and periodic review of technical accuracy of the age assurance process, some services stated that they regularly retrain or rerun age assurance models,²⁵⁷ carry out testing prior to releasing updates,²⁵⁸ or track performance metrics such as precision and recall on an ongoing basis.²⁵⁹
- A2.11 Services that rely on third-party age assurance providers,²⁶⁰ and particularly pornography services, typically relied on vendor-led monitoring and reporting, such as performance dashboards, regular reporting cycles, or service review meetings.

Robustness

- A2.12 In our HEAA guidance, we defined robustness as the degree to which an age assurance method can correctly determine the age of a user in actual deployment contexts.²⁶¹
- A2.13 Overall, while most services recognised and addressed some obvious circumvention risks, fewer were able to evidence systematic testing or evaluation of how their systems perform across real-world contexts once deployed.

²⁵⁵ [X] response to our information notice issued 15 December 2025.

²⁵⁶ [X] response to our information notice issued 15 December 2025.

²⁵⁷ [X] 2 analysed services’ responses to our information notices issued 15 December 2025.

²⁵⁸ [X] response to our information notice issued 15 December 2025.

²⁵⁹ [X] 7 analysed services’ responses to our information notices issued 15 December 2025.

²⁶⁰ [X] 15 analysed services’ responses to our information notices issued 15 December 2025.

²⁶¹ Robustness is covered in paragraph 4.44- 4.60 of the Part 5 HEAA guidance; paragraph 4.22 – 4.37 of the Part 3 HEAA guidance.

Testing in multiple environments

- A2.14 Some services described conducting testing in different environments to assess how age assurance systems perform under varying conditions, including different device types,²⁶² cameras or images of different quality,²⁶³ and real-world conditions such as differing lighting.²⁶⁴ Where referenced, this testing was usually described as part of broader quality assurance or reliability processes rather than as a clearly defined or standardised requirement.
- A2.15 Other services referred primarily to independent certification or made high-level statements about testing, without explicitly describing testing across multiple deployment environments. Limited patterns were observable: larger social media services were more likely to describe testing across conditions, while services relying more heavily on third-party age assurance providers more often cited vendor testing or certification instead.

Mitigating against circumvention

- A2.16 Most services provided some level of detail on steps taken to mitigate circumvention, with a common emphasis on preventing spoofing and limiting repeated trial-and-error attempts.
- A2.17 As explained in our HEAA guidance, liveness detection is used to ensure that the face being analysed is not a photograph, video, or any other form of spoofed representation. It provides further confidence that a child user has not circumvented the age check by uploading a photo of an adult, for example. Among the 29 services using facial age estimation, 25 explicitly referenced the use of liveness detection as a core control to mitigate spoofing risks, such as the use of photographs or pre-recorded videos. Of the remaining four services, two indicated that they use video selfies which is a form of liveness detection though not explicitly stated and the other two services are exploring the introduction of liveness detection.²⁶⁵
- A2.18 Services also described the use of retry limits,²⁶⁶ cooldown periods between attempts,²⁶⁷ and the removal of methods following repeated failures.²⁶⁸ These measures demonstrate awareness of basic circumvention patterns and are intended to reduce trial-and-error behaviour, even where services did not provide evidence of structured or real-world circumvention testing.
- A2.19 Pornography services, which were generally more likely to rely on credit card checks than other service types, described multiple safeguards to reduce the risk of circumvention. These included confirming that cards are credit rather than debit and the use of 3-D Secure authentication to confirm that the user has control of the card account.²⁶⁹

²⁶² [X] response to our information notice issued 15 December 2025.

²⁶³ [X] 6 analysed services' responses to our information notices issued 15 December 2025.

²⁶⁴ [X] 6 analysed services' responses to our information notices issued 15 December 2025.

²⁶⁵ [X] 2 analysed services' responses to our information notices issued 15 December 2025.

²⁶⁶ [X] 3 analysed services' responses to our information notices issued 15 December 2025.

²⁶⁷ [X] response to our information notice issued 15 December 2025.

²⁶⁸ [X] 11 analysed services' responses to our information notices issued 15 December 2025.

²⁶⁹ [X] 2 analysed services' responses to our information notices issued 15 December 2025.

- A2.20 The majority of services stated that they do not routinely repeat age checks for active UK users, with multiple services citing that this was not considered necessary or proportionate in normal circumstances. This is typically justified by reliance on a persistent binary output stored against the user account, or by requiring re-authentication with an age assurance provider rather than repeating the underlying verification.
- A2.21 Some analysed services reported selective repetition of age checks where specific risk signals or changes in user behaviour arise.²⁷⁰ This reflects an event-driven approach to repeat checking rather than routine or scheduled re-verification of all users.
- A2.22 Finally, services using age inference models differ materially from point-in-time age checks. Some rerun models periodically or on an ongoing basis rather than relying on a one-time determination of age/age range. One social media service stated that its age prediction models run continuously, producing an initial predicted age over an initial time period, with predictions subsequently refreshed on a regular basis, allowing age-related protections to adapt over time.²⁷¹
- A2.23 Several services reported making use of user reporting mechanisms that allow users to flag accounts suspected of being used by a user under 18.²⁷² These reports may trigger further review, account restrictions, or additional age assurance steps.

Reliability

- A2.24 In the HEAA guidance, we defined reliability as the degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.²⁷³
- A2.25 In general, services demonstrated mixed regard for reliability, and the concept was not always consistently interpreted by services. While many services referenced testing, certification, or provider assurances, fewer clearly articulated how reproducibility is monitored in live deployment or how data inputs are validated on an ongoing basis.
- A2.26 Testing, training, monitoring approaches that rely on artificial intelligence or machine learning
- A2.27 Services using artificial intelligence or machine learning methods such as facial age estimation and age inference generally described pre-deployment testing frameworks intended to assess consistency and reproducibility of outputs, most often within controlled environments.
- A2.28 One service reported testing models against labelled or benchmark datasets during development, enabling identical inputs to be re-run to confirm the stability of outputs over time.²⁷⁴ Other services primarily relied on external, independent testing and certification, stating that these assessments demonstrate predictable and consistent behaviour across standardised conditions.²⁷⁵

²⁷⁰ [3<] 3 analysed services' responses to our information notices issued 15 December 2025.

²⁷¹ [3<] 2 analysed services' response to our information notices issued 15 December 2025.

²⁷² [3<] 10 analysed services' responses to our information notices issued 15 December 2025.

²⁷³ Reliability is covered in paragraph 4.61 - 4.74 of the Part 5 HEAA guidance; paragraph 4.38 – 4.50 of the Part 3 HEAA guidance.

²⁷⁴ [3<] response to our information notice issued 15 December 2025.

²⁷⁵ [3<] 13 analysed services' responses to our information notices issued 15 December 2025.

- A2.29 Four services using proprietary facial age estimation technology stated that their system architecture is deterministic, producing the same output for the same input.²⁷⁶
- A2.30 A number of services reported conducting internal quality assurance activities, including review of model performance, testing changes prior to deployment, and internal monitoring of age assurance outcomes.²⁷⁷ These activities were often described as a way of identifying errors, assessing consistency, and improving processes over time.
- A2.31 One service described the use of anomaly monitoring to identify unusual patterns or outcomes in age assurance results, with the aim of detecting potential failures, abuse, or emerging risks.²⁷⁸

Ensuring that data is derived from a trustworthy source

- A2.32 To demonstrate that data used within the age assurance process is legitimate and derived from trustworthy sources, services described a range of checks, with approaches varying notably by method and service type.
- A2.33 A smaller number of services stated that they, or their third-party age assurance providers, only accept government-issued identity documents²⁷⁹ and/or conduct authenticity checks on those documents as part of photo-ID matching.²⁸⁰ However, this level of detail was absent from most responses where photo-ID matching was listed as a method, with limited explanation of how document legitimacy or circumvention risk is assessed in practice.
- A2.34 Where services used email-based age estimation, one service explained that its age assurance provider relies on digital identity data from trusted organisations, including banks, mortgage lenders and utility companies, in order to ensure that underlying data sources are reliable and resistant to fraudulent use.²⁸¹

Fairness

- A2.35 In the HEAA guidance, we defined fairness as the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.²⁸²
- A2.36 In general, services demonstrated clear regard for fairness, although the level of supporting evidence varied. In particular, most services recognised the importance of assessing the performance of certain age assurance methods (e.g. facial age estimation) across demographic groups, and several referenced demographic testing,²⁸³ or retraining models in some cases specifically where disparities were identified.²⁸⁴

²⁷⁶ [3<] 4 analysed services' responses to our information notices issued 15 December 2025.

²⁷⁷ [3<] 8 analysed services' responses to our information notices issued 15 December 2025.

²⁷⁸ [3<] response to our information notice issued 15 December 2025.

²⁷⁹ [3<] 2 analysed services' responses to our information notices issued 15 December 2025.

²⁸⁰ [3<] response to our information notice issued 15 December 2025.

²⁸¹ [3<] response to our information notice issued 15 December 2025.

²⁸² Fairness is covered in paragraph 4.75-4.82 of the Part 5 HEAA guidance; paragraph 4.51 -4.61 of the Part 3 HEAA guidance.

²⁸³ [3<] 16 analysed services' responses to our information notices issued 15 December 2025.

²⁸⁴ [3<] 2 analysed services' responses to our information notices issued 15 December 2025.

- A2.37 However, we have concerns about the number of services that are not yet providing service-level evidence of demographic fairness, particularly where reliance is placed on third-party provider testing without visibility of underlying datasets or their representativeness.

Diversity of testing and training datasets

- A2.38 Several services stated that their age assurance models were trained on or evaluated against datasets intended to reflect diversity across age, gender, ethnicity and/or geography.²⁸⁵ One large service provider described constructing evaluation datasets and processes designed to be statistically representative of its user base, which are used to assess “sub-population” performance as part of model validation.²⁸⁶
- A2.39 Some services also referenced the use of industry-standard datasets commonly applied in the evaluation of facial analysis systems, with some services noting that these are intended to expose models to a wide range of faces and age groups and support assessment of performance across demographic cohorts.²⁸⁷
- A2.40 Two services reported accuracy metrics broken down by demographic attributes, such as true positive rates across gender, skin tone, or age bands.²⁸⁸ Where variation was observed, services generally stated that differences were modest and did not materially affect overall system performance. In a small number of cases where discrepancies were identified, services described this as prompting opportunity for further retraining, reviewing, or refinement of models.²⁸⁹ For example, one service provider noted differences in precision by demographic group, which it stated led to an opportunity for additional retraining and evaluation.²⁹⁰
- A2.41 Several services relied on demographic testing undertaken by their third-party age assurance provider, without providing visibility of underlying datasets or sampling methodologies.²⁹¹ While such testing provides some assurance that models are evaluated for bias, the evidence provided lacked detail about the underlying datasets and how representative they are of UK users, as well as the sampling methodologies.
- A2.42 Some services highlighted the role of user appeals and complaints processes as a means of identifying errors or weaknesses in age assurance outcomes.²⁹² Appeals processes were described as enabling users to challenge age determinations and, in some cases, prompting manual review or reassessment of the age assurance result. In Section 8 we highlight that services should implement an effective appeals process and monitor and investigate appeals as needed.

²⁸⁵ [3<] 15 analysed services’ responses to our information notices issued 15 December 2025.

²⁸⁶ [3<] 2 analysed services’ responses to our information notices issued 15 December 2025.

²⁸⁷ [3<] 4 analysed services’ responses to our information notices issued 15 December 2025.

²⁸⁸ [3<] 2 analysed services’ responses to our information notices issued 15 December 2025.

²⁸⁹ [3<] 5 analysed services’ responses to our information notices issued 15 December 2025.

²⁹⁰ [3<] 3 analysed services’ responses to our information notices issued 15 December 2025.

²⁹¹ [3<] 3 analysed services’ responses to our information notices issued 15 December 2025.

²⁹² [3<] 8 analysed services’ responses to our information notices issued 15 December 2025.

Additional principles for providers to consider

- A2.43 As well as being highly effective, in our HEAA guidance we stated that the age assurance process should be easy to use and work for all users, to ensure that adult users are not unduly prevented from accessing legal content. We therefore advised that, alongside fulfilling the criteria, service providers should also consider the principles of **accessibility** and **interoperability**.

Accessibility

- A2.44 In our HEAA guidance, we defined accessibility as the principle that age assurance should be easy to use and work for all users, regardless of their characteristics or whether they are members of a certain group.²⁹³
- A2.45 Overall, services demonstrated that they had considered accessibility in the design and implementation of their age assurance processes, particularly through offering multiple methods and user support features. Services recognise the importance of ensuring that age assurance is easy to use and works for all users. To go further, services could carry out more detailed impact assessment or consideration of accessibility across the full end-to-end user journey.
- A2.46 One service acknowledged that relying solely on a single age assurance method can disadvantage some users, including those without access to formal identity documents.²⁹⁴ Most services stated that they offer a range of age assurance methods and fallback options for accessibility reasons.²⁹⁵ Only five services reported offering just one age assurance method.²⁹⁶
- A2.47 Some services referred to providing supporting information to help users complete age checks, including simple instructions or help articles written in plain English.²⁹⁷ Some services reported that their age assurance providers user flows met recognised accessibility standards.²⁹⁸ Many services stated that their age assurance processes are compatible with assistive technologies such as screen readers or voice commands.²⁹⁹ One service reported conducting a formal accessibility audit via a third-party provider and subsequently making changes to improve accessibility,³⁰⁰ while others stated that customer service or human review is available where users experience difficulty completing age assurance.³⁰¹
- A2.48 Services generally reported notifying users of when age assurance is required, including informing them about the purpose of the age checks, particularly for porn services who use age assurance to prevent access to users determined to be children. Social media services that use age inference to generate estimates of users' ages in the background tended to

²⁹³ Accessibility is covered in paragraph 4.86 -4.91 of the Part 5 HEAA guidance; paragraph 4.62- 4.67 of the Part 3 HEAA guidance.

²⁹⁴ [redacted] response to our information notice issued 15 December 2025.

²⁹⁵ [redacted] 13 analysed services' responses to our information notices issued 15 December 2025.

²⁹⁶ [redacted] 5 analysed services' responses to our information notices issued 15 December 2025.

²⁹⁷ [redacted] 6 analysed services' responses to our information notices issued 15 December 2025.

²⁹⁸ [redacted] 4 analysed services' responses to our information notices issued 15 December 2025.

²⁹⁹ [redacted] 14 analysed services; responses to our information notices issued 15 December 2025.

³⁰⁰ [redacted] response to our information notice issued 15 December 2025.

³⁰¹ [redacted] 13 analysed services' responses to our information notices issued 15 December 2025.

state that users are made aware of its use but generally did not specify how or where this information is presented within the user journey.³⁰²

- A2.49 Other elements identified by services that are supportive of accessibility included the availability of multiple language options,³⁰³ compatibility across a range of devices and/or browsers,³⁰⁴ the absence of a requirement for specialised equipment.³⁰⁵

Interoperability

- A2.50 In our HEAA guidance, we defined interoperability as the ability for technological systems to communicate with each other using common and standardised formats.³⁰⁶
- A2.51 In general, most services are not yet using interoperable or reusable age credentials, and in part this is because these approaches were not widely available at the point at which services were required to implement age assurance. However, evidence suggests that there is increasing experimentation and investment, particularly at the account and operating-system layer, as well as with digital-identities, which may support wider use of interoperable age credentials over time.
- A2.52 Two large social media services stated that age signals associated with a user account can be applied consistently across connected services within their ecosystems.³⁰⁷
- A2.53 Most services do not currently rely on interoperable or reusable age credentials. Some of the pornography services using Digital-ID did mention reusability, with one service describing the use of an interoperable age token issued by its third-party provider, which can be reused across that provider's partner network.³⁰⁸ They highlighted that this allows users to verify their age once to access multiple services.
- A2.54 Multiple services stated that they are monitoring developments in digital identity and/or interoperable solutions, showing openness to adopting interoperable age credentials.³⁰⁹ One large social media service outlined its intent to potentially integrate with a third party service to facilitate and enable reuse of age verification across services via cryptographically secure tokens.³¹⁰
- A2.55 Since July 2025, wider industry developments indicate that efforts to achieve greater interoperability within the age assurance ecosystem are growing. These developments include the provision of reusable age credentials by third-party providers, the use of zero-knowledge proofs to confirm age without disclosing identity, and the introduction of operating-system or account-level age checks for UK account holders.³¹¹

³⁰² [3] 4 analysed services' responses to our information notices issued 15 December 2025.

³⁰³ [3] 5 analysed services' responses to our information notices issued 15 December 2025.

³⁰⁴ [3] 5 analysed services' responses to our information notices issued 15 December 2025.

³⁰⁵ [3] 4 analysed services' responses to our information notices issued 15 December 2025.

³⁰⁶ Interoperability is covered in paragraph 4.92 -4.97 of the Part 5 HEAA guidance; paragraph 4.68 -4.73 of the Part 3 HEAA guidance.

³⁰⁷ [3] 3 analysed services' responses to our information notices issued 15 December 2025.

³⁰⁸ [3] response to our information notice issued 15 December 2025.

³⁰⁹ [3] 3 analysed services' responses to our information notices issued 15 December 2025.

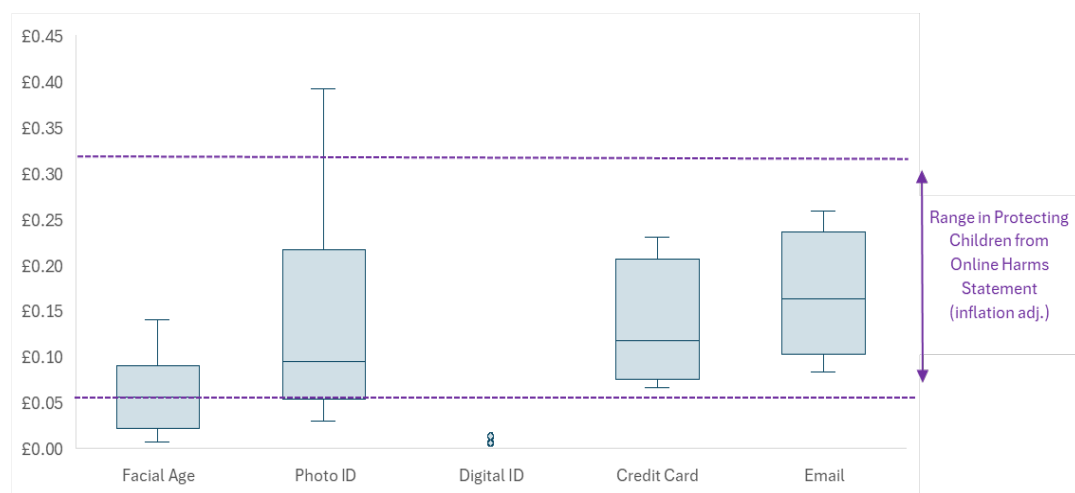
³¹⁰ [3] 2 analysed services' responses to our information notices issued 15 December 2025.

³¹¹ From AVPA: [Interoperable Age Assurance](#).

A3. Cost and choice of age assurance methods

- A3.1 As discussed in Section 7, the average per-check cost incurred by the service providers we analysed does not appear high. It generally sits towards the lower end of the range of £0.05 to £0.30 we provided in our April 2025 Statement, where we estimated per-check cost figures in the range of £0.05 to £0.30.³¹²
- A3.2 We also looked at the analysed service providers' cost of checking users by method. As shown in Figure 13, the information notice evidence shows some variation in per-check cost figures across methods and across service providers using the same method. However, differences appear relatively limited overall: cost ranges generally fall within the range published in our April 2025 Statement, with most median costs sitting towards the lower end of it.³¹³

Figure 13: Distribution of estimated average per-check cost by method incurred by the analysed service providers.



Note: Per-check cost ranges for MNO, open banking and age tokens are not included in the chart due to confidentiality considerations arising from small sample sizes. The submitted costs for these methods are within, or below, the range set out in our April 2025 Statement.

Source: Services' responses to our information notice issued 15 December 2025.

- A3.3 The only exception is photo ID matching. Although the median price for this method is low, data reported by a small number of analysed social media service providers implied per-check cost figures slightly above the upper end of the range.³¹⁴ Digital ID checks are offered by 12 analysed services and are generally reported to be available free of charge,³¹⁵ with two services reporting only minimal costs.³¹⁶

³¹² Volume 5 Annex. Paragraph A3.30, Page 9.

³¹³ [3<] 16 analysed service providers' responses to our information notices issued 15 December 2025 (excluded from analysis for lack of data: [3< 3 analysed service providers'].

³¹⁴ [3<] 2 analysed service providers' responses to our information notices issued 15 December 2025.

³¹⁵ [3<] 9 analysed service providers' responses to our information notices issued 15 December 2025.

³¹⁶ [3<] 2 analysed service providers' responses to our information notices issued 15 December 2025.

Variation in costs likely reflect factors such as, for example, underlying technology, provider pricing models, implementation choices, commercial dynamics, and wider market conditions. For example, facial age estimation and photo ID matching appear to be the most used methods, which may have helped reduce their prices on average.

- A3.4 However, the available evidence does not suggest that cost was generally the primary factor shaping the age assurance methods adopted by analysed service providers. Where service providers explained their choice, they commonly pointed to factors such as compliance, effectiveness, accuracy, privacy, and user experience.³¹⁷ Several analysed service providers said that cost was considered, usually as part of a broader assessment or as secondary to these other factors.³¹⁸ Some analysed service providers stated more directly that cost did not influence their decision, was not a determining factor, or was not the primary factor in shaping their approach to age assurance.³¹⁹
- A3.5 This is consistent with analysed services offering multiple age assurance methods, often via more than one third-party provider, as discussed in Section 1. This suggests costs was unlikely to be a primary barrier to offering a range of approaches for the analysed service providers.
- A3.6 In addition, as mentioned in paragraph 7.15, third-party provider pricing structures vary. While some providers price methods differently, others may offer bundled solutions and charge per check regardless of the method used. Where such models are offered, this may reduce the influence of cost differences on service choices.

³¹⁷ [3] 16 analysed service providers' responses to our information notices issued 15 December 2025.

³¹⁸ [3] 13 analysed service providers' responses to our information notices issued 15 December 2025. In particular, cost influenced some decisions. For example, some analysed service providers referred to cost when assessing whether to rely on third-party age assurance providers or build a proprietary solution [3] 3 analysed service providers], considering scalability or operational feasibility [3] 4 analysed service providers], or, in one case, deciding not to use a particular method [3].

³¹⁹ [3] 5 analysed service providers' responses to our information notices issued 15 December 2025.

A4. Glossary

Abbreviation, word or phrase	Meaning
The Act	The Online Safety Act 2023.
Active UK user	Active United Kingdom (UK) users for the purpose of this report are users located in the UK who have accessed the user-to-user part of a regulated user-to-user service.
Age assessment appeals process	A complaint by a United Kingdom user who is unable to access content because measures used to comply with a duty set out in section 12(2) or (3) of the Act have resulted in an incorrect assessment of the user's age.
Age assurance (AA)	A collective term for age verification and age estimation as defined in section 230 of the Act.
Age assurance method	The particular 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 whether or not a user is a child.
Age check	An individual instance of an age assurance process being applied to a user.
Age estimation	Any measure designed to estimate the age or age range of users of a regulated service. ³²⁰
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. ³²¹
Age verification	A form of age assurance designed to verify the exact age of the user. ³²²
Blur gate	An age assurance approach in which users see a series of blurred images before the age check. In some cases, titles are visible which could contain strong sexual wording. Clicking on a thumbnail directs users to an age check.
Call for Evidence (CfE)	Online safety regulation: Statutory reports on age assurance and app stores, published 3 November 2025

³²⁰ Section 230(3) of the Act.

³²¹ See 'Age inference models' Statement: Age Assurance and Children's Access, 16 January 2025.

³²² Section 230(2) of the Act.

Circumvention	Actions taken by a user to pass through an age gate without confirming their age. This can be done in a number of ways including: (a) bypass or attempt to bypass the age gate all together e.g. by using a VPN; (b) misrepresenting their age; or (c) using another person's credentials.
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 exact age of the user before determining whether the user is a child.
Check costs	Costs incurred by a service to check the user base.
Children's access assessment	A process that all Part 3 services in scope of the Act must carry out to determine whether they are likely to be accessed by children.
Configuration settings	Adjustable options that determine how a system operates. In the context of an age assurance solution, configuration settings are settings that allows services to tailor specific features of the solution to change how it operates, such as to turn on or off liveness detection.
Content harmful to children	a) Primary Priority Content (PPC);³²³ b) Priority Content (PC);³²⁴ and c) content, not within paragraph (a) or (b) which presents a material risk of significant harm to an appreciable number of children in the UK, referred to as 'non-designated content that is harmful to children' (NDC).³²⁵
Digital identity services	Systems that provide a reusable way for users to prove their age or identity across multiple interactions and transactions. A digital identity is a digital representation of a person which enables them to prove who they are online or in person. Reusable digital identities can be used multiple times and may include digital identity wallets, which enable users to verify and securely store attributes (such as age) in digital form and share specific attributes (e.g. age or confirmation of adulthood) with a relying party.
Direct costs	Costs incurred by a service in implementing and operating age assurance, including set-up costs, ongoing costs, and check costs where applicable.

³²³ Defined in Section 61 of the Act.

³²⁴ Defined in Section 62 of the Act.

³²⁵ Section 60(2 and (4)) of the Act.

Facial age estimation	An age estimation method that works by analysing the features of a user's face to estimate their age.
Fairness	The extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.
False negative	An outcome of an age assurance process in which an adult is incorrectly classified as a child.
False positive	An outcome of an age assurance process in which a child is incorrectly classified as an adult.
Front gate	An age assurance approach in which users see only a blank landing page, with no content visible until they have completed the age check.
Geo-blocking	A restriction applied by a service to prevent access from users in specific geographic locations, such as the United Kingdom.
Highly Effective Age Assurance (HEAA)	An age assurance process that is of such a kind and used in such a way that it is highly effective at correctly determining whether or not a particular user is a child.
Image gate	An age assurance approach in which users see a series of clearly visible images. Often these are of clothed people, sometimes in sexually suggestive poses and/or wearing lingerie. In some cases, titles are visible which could contain strong sexual wording. In some variations, users can see a preview of the video when hovering over with a cursor. Clicking on the thumbnail directs users to an age check.
Indirect costs	Impact on service revenue driven by changes in user behaviour, following the implementation of age assurance.
Information notice	A formal request issued by Ofcom under section 100 of the Act requiring a service provider to provide any information Ofcom may require for the purposes of exercising or deciding whether to exercise any of their online safety functions.
Interoperability	The ability for technological systems to communicate with each other using common and standardised formats.
In-video gate	An age assurance approach in which users see a series of thumbnails that contain clearly visible images. Often these are of clothed people, sometimes in sexually suggestive poses and/or wearing lingerie. In some cases, titles are visible which could contain strong sexual wording. Users can sometimes see a preview of the video when hovering over with a cursor. Users can then watch the video up until a certain point, usually up until nudity is shown, after which they are directed to an age check.

Liveness detection	A feature used to ensure that the facer 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.
Ongoing costs	Costs incurred by a service for running an age assurance solution.
Part 5 services	Service providers that display or publish pornographic content on their online services.
Photo ID matching	An age verification method that works by capturing relevant information from an uploaded photo-ID document and comparing it to an image of the user at the point of ID upload to verify that they are the same person.
Protection of Children Code	Ofcom's Code of Practice for user-to-user services, which sets out measures that those services can take to comply with their duties to protect children under the Act.
Provider ³²⁶	The provider of an internet service for the purposes of the Act that: • In the case of regulated user-to-user services, has control over who can use the user-to-user part of the service; or • In the case of regulated search services, has control over the operations of the search engine. Where no such entity exists, the provider will be the individual or individuals who have control over who can access the user-to-user part of the user service or who has control over the operations of the search service.
Proxy server	Intermediary servers which have the capability to make requests on behalf of a user/client.
Regulated service	A regulated user-to-user service, a regulated search service or a Part 5 service.

³²⁶ Section 226 of the Act.

	Services will be regulated if they have links with the UK, ³²⁷ and are not exempt. ³²⁸
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.
Search services	An internet service that is, or includes, a search engine. ³²⁹
Set-up costs	Costs incurred by a service for setting up an age assurance solution.
Technical accuracy	The degree to which an age assurance method can correctly determine the age of a user under test lab conditions.
Tor browser	A web browser that provides a route to access a network layer that re-routes internet traffic in such a way as to "anonymise" and obfuscate the origin and destination of web requests.
User migration	The movement of users from one service to another, for example from services with age assurance to those without it.
User-to-user services	An internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service. ³³⁰
Virtual private network (VPN)	The creation of a private network over a public internet connection.

³²⁷ A user-to-user or search service will have links with the UK if:

- it has a significant number of users in the UK;
- the UK is a target market; or
- it is capable of being used by individuals in the UK and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK because of the user-generated content present on the service or search content (as relevant). See Sections 4(5) and (6) of the Act.

A Part 5 online pornography service has links with the UK if:

- it has a significant number of users; or
- UK users form one of the target markets. See Section 80(4) of the Act.

³²⁸ For exempt user-to-user and search services, see Schedule 1 to the Act. Regulated user-to-user and search services do not include a service combining user-generated content or search content not regulated by the Act with pornographic content that is regulated (Section 4 of the Act).

For exempt Part 5 online pornography services, see Schedule 9 to the Act.

³²⁹ Section 3(4) of the Act.

³³⁰ Section 3(1) of the Act.

