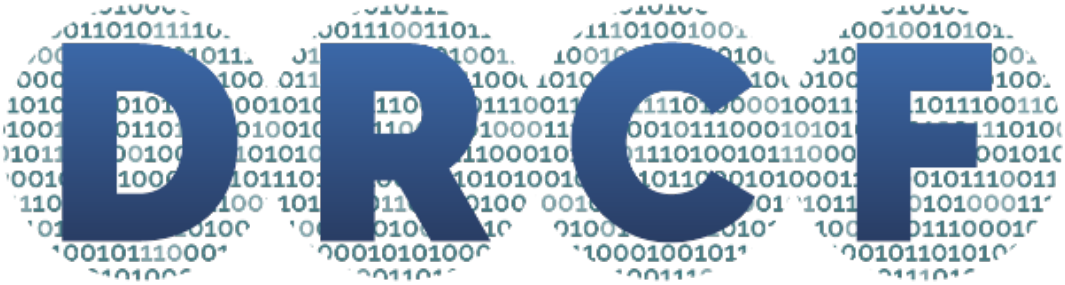

Digital Regulation Cooperation Forum

Ofcom ico. Information Commissioner's Office

Age Assurance

A Joint Statement by Ofcom and the Information Commissioner's Office

25 March 2026

1. Introduction

As the regulators responsible for online safety and data protection in the UK, Ofcom and the Information Commissioner's Office (ICO) are committed to creating a safe and secure online environment for people, especially children, to protect them from both harmful content and data harms online.

This joint statement[1] is aimed at services likely to be accessed by children and in scope of the Online Safety Act (OSA) and UK data protection legislation[2] which are implementing age assurance. Age assurance plays an important role in Ofcom and the ICO's shared goal of protecting children from harm online.

In this joint statement, we provide greater clarity on how you can meet your obligations under both the OSA and UK data protection legislation when implementing age assurance. Our approach is designed to be risk-based, flexible, tech-neutral and future-proof, allowing space for innovation in the context of rapidly evolving technology and market developments.

Scope of this joint statement

This joint statement outlines the main areas of interaction between online safety and data protection laws[3] as they relate to age assurance. It summarises key aspects of existing Ofcom and ICO age assurance policy in a practical way to help you comply with both your online safety and data protection obligations.

Annex A provides a high-level summary of requirements under both OSA and data protection legislation, and includes references to relevant Ofcom and ICO publications for further detail.

[1] We previously published two joint statements: our 2022 joint statement, which set out shared vision for a clear, coherent regulatory landscape for online services; and our 2024 joint statement, which outlined our ways of working.
[2] The statement reflects the updated data protection requirements for services handling children's data in accordance with the DUA Act 2025.
[3] This relates to the UK Online Safety Act 2023 and data protection law. In this statement, data protection law refers specifically to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

2. Age assurance expectations

What does this section cover?

This section summarises the regulatory requirements under the OSA and data protection legislation that apply when you implement age assurance on your service. It includes:

- Our common approach to age assurance
- Your age assurance obligations under the Online Safety Act
- Your age assurance obligations under data protection law

Our common approach to age assurance

Our approaches to age assurance and regulatory expectations align in a number of ways:

- If you are implementing age assurance, you must choose the most appropriate method to reduce risks and potential harms to children online. We share a **flexible, tech-neutral approach**.
    - Where your service falls in scope of the OSA age assurance duties, you must have an age assurance process that is highly effective at determining whether or not a user is a child.[4]
    - If you set a minimum age for your service, you should use an effective age gate to prevent underage access and avoid unlawful processing under UK GDPR.
- We agree that **self-declaration alone is not an effective means** to determine the age or age range of users and prevent access by underage users.[3]
- We recognise that **all age assurance methods involve the processing of personal data**. You can process personal data for age assurance, as long as the method you use is necessary, proportionate to your risks, and complies with data protection legislation.[5]
- We agree that **age assurance methods must address risks of circumvention** that would impact on the accuracy and robustness of the methods.
- We **do not expect you to use age assurance methods that are not technically feasible** or that introduce risks to rights and freedoms that outweigh the benefits. These considerations are already reflected in our existing requirements and guidance.

[4] For more details, see Ofcom's Guidance on highly effective age assurance for Part 3 services.
[5] See the ICO's Age assurance Opinion - Expectations for age assurance and data protection compliance.

Your age assurance obligations under the Online Safety Act

Under the OSA, if you are a user-to-user service[6] that is likely to be accessed by children and allows harmful content known as primary priority content,[7] or if you are a service that publishes or displays its own pornographic content,[8] **you must use highly effective age assurance (HEAA) to prevent children from encountering such content**. Ofcom's Protection of Children Code for user-to-user services[9] also recommends age assurance measures to protect children from other harmful content[10] and from harmful features, functionalities or behaviours.

Ofcom's guidance on HEAA[11] sets out **four criteria** that your age assurance process should fulfil to be considered highly effective, as well as **two principles** you should have regard to in order to ensure it is **easy to use and works for all users**. Failing to do so might unduly prevent adult users from accessing legal content. See Figure 1 for the HEAA criteria and principles.

Figure 1. Criteria and principles of highly effective age assurance

Ofcom's guidance gives your service some **flexibility to choose age assurance method(s)** that are appropriate to your specific context, including size, user base, and available resources, provided you can demonstrate that these meet the requirements of the OSA.

Methods that Ofcom considers **capable of being highly effective** at determining whether a user is a child include, but are not limited to, the list shown in Figure 2. Ofcom is also clear that certain

[6] Services regulated under Part 3 of the OSA, see also section 4 for further details on the definition of a regulated service.
[7] Primary priority content includes pornography, self-harm, suicide and eating disorder content as set out in section 61 of the OSA.
[8] Services regulated under Part 5 of the OSA.
[9] Protection of Children Code of Practice for user-to-user services.
[10] Priority content and non-designated content as set out in sections 60 and 62 of the OSA.
[11] Guidance on highly effective age assurance part 3 guidance; Guidance on highly effective age assurance and other Part 5 duties.

methods are **not capable of being highly effective**: self-declaration of age when used in isolation,[12] age verification through online payment methods which do not require the user to be 18 or over (e.g. debit cards) and general contractual restrictions on the age of users on your service.[13]

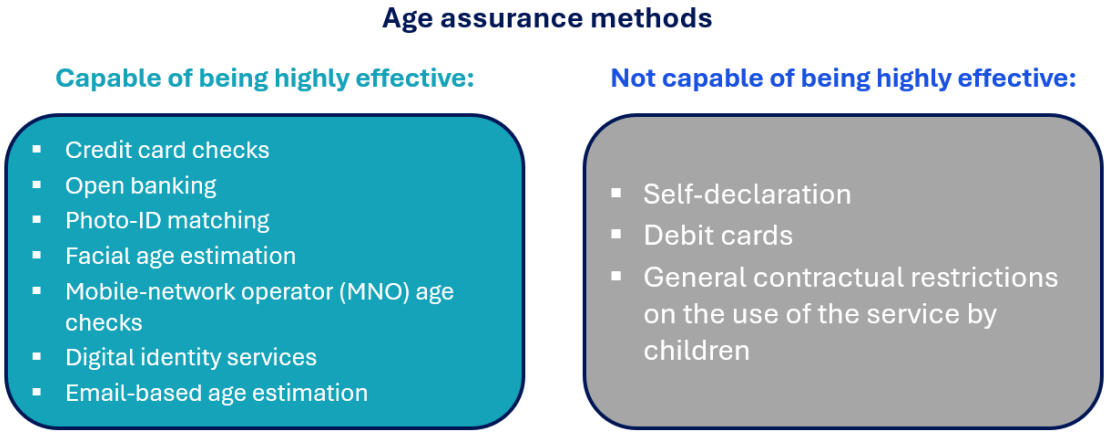

Figure 2. Non-exhaustive list of methods which are and are not capable of being HEAA

You should take steps, where possible, to **mitigate against circumvention** methods. This means choosing an age assurance method that sufficiently guards against fake input and binds the proof of age to the user presenting for the age check.

The OSA does not require you to set a minimum age to access your service. However, if you choose to do so, you must explain this in your terms of service and apply it consistently. You do not need to use HEAA to prevent children under your minimum age from accessing your service. However, if you do not, you should assume that underage children are present on your service. You will need to take account of this in your children's risk assessment and deploy the necessary protections to ensure that your service is appropriate for all children. These steps are necessary to demonstrate compliance with your duties to protect children from harmful content online under the OSA. Where you do not take these steps, Ofcom may investigate and take enforcement action if necessary.

Beyond these compliance requirements, we have recommended that if you are a service most used by children, you should use HEAA to enforce your minimum age policies effectively.[14] Given significant underage use of your service, we expect you to take robust measures, including HEAA, to identify and protect underage children from harm.

[12] As set out in s230(4) of the OSA.
[13] For example: including as part of the terms of service a condition that prohibits users who are under 18 years old from using the service, without any additional age assurance; general disclaimers asserting that all users should be 18 years of age or over; or warnings on specific content that the content is only suitable for over 18s.
[14] Keep underage children off your platforms, Ofcom tells tech firms.

Your age assurance obligations under data protection legislation

Age assurance plays a crucial role in helping to protect children from harmful data processing. It can help organisations protect children's personal information, and support compliance with your legal obligations by ensuring that you can:

- avoid unlawfully processing children's data by identifying children who are under your minimum age and preventing them access to your service; and
- determine any child users that are allowed to access your service so you can put in place the appropriate protections in the Children's code.

If you are using age assurance to comply with these obligations under data protection law, then you must ensure that the age assurance method you choose is necessary, **effective for your purposes and proportionate to level of risk on your service.** You must also ensure that whatever method you choose, this complies with UK GDPR data protection principles.

Preventing underage access

Where you are operating a service that is not suitable for children under a certain age, your focus should be on **preventing underage children from accessing your service**. This includes where you have set a minimum age in your terms of service, such as 13. This is because you will generally have no lawful basis for processing the personal data of children who are not meant to be on your service.[15]

The best way to prevent access to underage children and minimise the risk of unlawful processing is to implement an effective age gate. The ICO does not mandate the use of any specific technologies but expects services to use appropriate, current viable technologies when enforcing minimum age requirements. For services enforcing a 13 minimum age, current examples include, but are not limited to, facial age estimation, digital ID, or one-time photo matching.

Self-declaration is not an effective form of age assurance to prevent access to underage users because it can be easily circumvented. In reviewing current industry use of profiling[16] for age assurance, the ICO considers that it is also not currently an effective method for preventing underage users from accessing a service that is unsuitable for them.

Where there is a risk of unlawful processing, as described above, you should address this through an alternative age assurance method.

---

[15] Refer to the ICO's lawful basis guidance for more information.

[16] Under UK data protection law, profiling is defined as: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

Children's code protections

Where you are operating a service that is suitable for children or children above a certain age, your focus must be on ensuring that their experience is age-appropriate, in line with the ICO's Children's code. You can do this by using age assurance methods which are proportionate to the risks on your platform that provide sufficient confidence to apply the standards according to the user's age.

The ICO's Age Assurance Opinion explains how you can use age assurance technology in compliance with data protection law in a risk-based and proportionate way. If your personal information processing activities are likely to present a high risk[17] to children's rights and freedoms, you should introduce age assurance methods that give the highest possible level of certainty on a user's age.

If you don't have a level of certainty about the age of your users that is appropriate to the risks to children arising from your data processing, you must apply the Children's code standards to all users. This guarantees that children receive essential data protection safeguards even where their age cannot be reliably confirmed.

This approach does not require you to disregard age information you already hold. Instead, it provides a default baseline of protection. You should still apply the code in a way that reflects the age information available to you, while acknowledging that it is not sufficiently reliable.

Data protection principles

You can process personal data for age assurance, as long as the method you use is necessary, proportionate to your risks and complies with data protection principles. Regardless of which age assurance technologies or process you adopt and whether you are processing a child's or adult's personal information, you **must** follow the data protection principles in Figure 3.

[17] High-risk processing includes but is not limited to large-scale profiling of children, targeting children for marketing and advertising. The ICO has published guidance on data processing activities that are considered "likely to result in high risks"

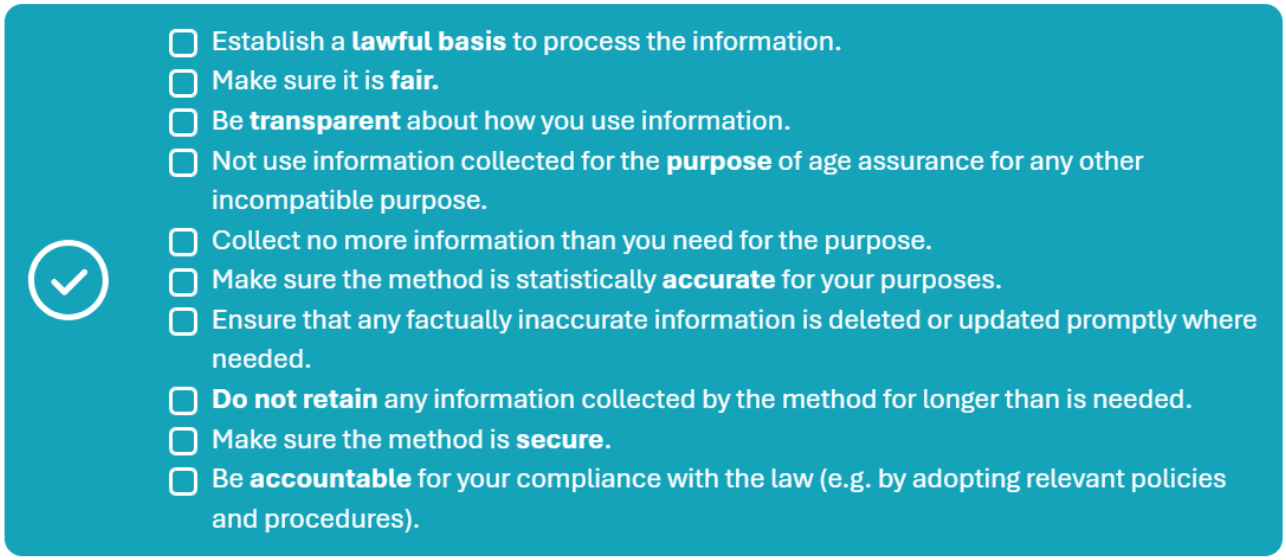

Figure 3. UK GDPR data protection principles

You can find more information on applying data protection principles to your chosen age assurance approach in the ICO's Age Assurance Opinion. To support compliance, the ICO has worked with industry to develop approved data protection certification schemes. You can use the Age Check Certification Scheme to help you identify age assurance providers that meet UK data protection standards.

3. Practical examples

This section includes two hypothetical examples to help you understand how you can implement an age assurance process that meets both online safety and data protection requirements in practice.

Our approach offers you some flexibility in how you implement age assurance, for example in choosing methods that are suitable for your own services and users. The details in this section are illustrative and should not be read as endorsing a particular method or process.

You should refer to our guidance when deciding what is the most appropriate method and process for your service to ensure compliance. See Annex A for more details.

Example 1: User-to-user pornography service

Sector	Pornography
Context	A pornography service that is available in the UK and is likely to be accessed by children hosts user-generated pornographic content. It is a Part 3 user-to-user service under the OSA. As the service allows pornographic content in its terms of service, it must ensure that children are prevented from encountering such content on its service.

Approach to comply with OSA obligations	Approach to comply with data protection obligations
To meet its obligations under the OSA, the service takes the following steps: 1. **It puts in place a highly effective age assurance process.** The methods chosen fulfil the criteria and have regard to the principles outlined in Ofcom's part 3 HEAA guidance. The service can demonstrate that the methods chosen have been implemented in such a way that ensures the process as a whole is highly effective. 2. **It ensures no pornographic content is accessible before the user has completed an age check.** This applies for both logged-in and logged-out users.[18] 3. **It takes steps where possible to reduce the risk of circumvention.** The service considers circumvention as part of implementing an age assurance process that is robust.	To meet its obligations under data protection law, the service takes the following steps: 1. **It establishes a lawful basis to process the information.** The service relies on legal obligation for age assurance as it is required under the OSA. 2. **It applies all data protection principles to its age assurance technology or process it adopts**. The service applies all the data protection principles to its age assurance. In line with the principle of data minimisation, storage limitation, and purpose limitation, it collected only the information strictly necessary to confirm a user's age or age range. 3. **It is transparent about how it uses information.** The service provides users with clear and accessible privacy notices that explain why age assurance was required, what data would be collected, how long it would be stored, and how users could exercise their data protection rights. 4. **It makes sure its age assurance processes are fair.** The service provides tools so that users can challenge inaccurate age assurance decisions. It makes this accessible and prominent, so people can exercise their data protection rights easily. 5. **It is accountable for its compliance with the law.** The service continues to review the risks and effectiveness of its age assurance methods to ensure they remain appropriate and update its DPIA if new data protection risks emerge.

[18] For further information, see Ofcom's Age checks: Why their placement matters in pornography.

Example 2: Social media service

Sector	Social media
Context	A large social media service that is available in the UK and is likely to be accessed by children hosts a wide range of user-generated content. It is a Part 3 user-to-user service under the OSA. While the service is not dedicated to the hosting and sharing of content harmful to children, it offers a Not Safe For Work (NSFW) section, where content harmful to children is allowed, such as pornography. The service offers both a logged-in and a logged-out experience, and specifies a minimum age of 13 in its terms of service.

Approach to comply with OSA obligations	Approach to comply with data protection obligations
To meet its obligations under the OSA, the service takes the following steps: 1. **It puts in place a highly effective age assurance process**. The methods chosen fulfil the criteria and have regard to the principles outlined in Ofcom's part 3 HEAA guidance. The service can demonstrate that the methods chosen have been implemented in such a way that ensures the process as a whole is highly effective. 2. **It ensures users that have not been determined to be an adult by highly effective age assurance are protected from harmful content.** Logged-out users and logged-in users who have not completed an age check cannot access the NSFW section. Content remains inaccessible unless the user is confirmed to be an adult using HEAA. 3. **It takes steps where possible to reduce the risk of circumvention.** The service considers circumvention as part of implementing an age assurance process that is robust. 4. **It applies the minimum age stated in its terms of service effectively, as per Ofcom's recommendation.** The service has chosen to include a minimum age of 13 in their terms of service. Since it is one of the services most used by children, it uses HEAA to enforce its minimum age policy effectively. 5. **It measures and monitors ongoing performance.** The service regularly monitors and measures against key performance indicators of the system on an ongoing basis.	To meet its obligations under data protection law, the service takes the following steps: 1. **It is accountable for its compliance with the law.** As part of meeting its accountability obligations, the service conducts a DPIA to evaluate the risks associated with its data processing activities. 2. **It applies robust age assurance where it does high-risk processing and has a minimum age in its terms of service.** The service has a minimum age of 13 in its terms of service. It is therefore unlikely to have a lawful basis for processing the personal data of children under that age. The service deploys a robust age assurance method appropriate and proportionate to the level of data processing risk on its platform at the account creation stage to determine which users are under 13 and block them from accessing their platform. 3. **It applies all data protection principles to its age assurance technology or process it adopts**. The service applies all the data protection principles to its age assurance. In line with the principle of data minimisation, storage limitation, and purpose limitation, it collected only the information strictly necessary to confirm a user's age or age range. 4. **It is accountable for its compliance with the law.** The service continues to assess the risks and effectiveness of its age assurance approaches to ensure they remain fit for purpose.

4. Conclusion

Ofcom and the ICO are united in our goal to protect children from harm online. As set out in this joint statement, you need to use age assurance to prevent children from encountering harmful content and data harms online.

This joint statement aims to provide more clarity and practical examples to help you comply with both your online safety and data protection obligations. When implementing age assurance, you should consult the relevant Ofcom and ICO guidance to ensure the age assurance process you implement fulfils your online safety and data protection obligations.

We will continue to collaborate on this important area and respond to any future developments in age assurance, as appropriate.

Annex A – Summary of how to comply with the Online Safety Act and UK data protection legislation

Type of organisation	How to comply with the Online Safety Act	How to comply with UK data protection legislation
Online services that are likely to be accessed by children but are not in scope of the OSA	• No requirements under the OSA as it does not apply to your service.	• Ensure children's personal data is only processed where a valid lawful basis has been identified and where the processing would meet the requirements of fairness. • If your terms of service state that under 13s should not be accessing your services, you must ensure that you deploy robust age assurance mechanisms to prevent this from happening and minimise the risk of unlawful processing. • Establish age or age range with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your information processing or apply the standards in the Children's code to all your users instead. Self-dec alone is not appropriate if you are a high-risk service.
Online services that are likely to be accessed by children and are user-to-user services in scope of Part 3 of the OSA	• Refer to Ofcom's Guidance on highly effective age assurance to understand when and how to implement HEAA • Refer to recommended age assurance measures set out in Ofcom's Protection of Children Codes, (Measures PCU B1-PCU B7). • Refer to Section 3 of the Statement on Age Assurance and Children's Access to understand Ofcom's recommendations, including further technical detail to help you implement highly effective age assurance. • Stay across upcoming updates to Ofcom's illegal content codes, which will codify the use of highly effective age assurance to strengthen protections for children where they are at heightened risk of encountering illegal harms.	• Ensure children's personal data is only processed where a valid lawful basis has been identified and where the processing would meet the requirements of fairness. • If your terms of service state that under 13s should not be accessing your services, you must ensure that you deploy robust age assurance mechanisms to prevent this from happening and minimise the risk of unlawful processing • Establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your information processing or apply the standards in the Children's code to all your users instead.

Online services that allow pornographic content	Part 3 services • Use highly effective age assurance to prevent children from accessing pornographic content, following Ofcom's Guidance on highly effective age assurance for Part 3 services. • Refer to recommended age assurance measures set out in Ofcom's Protection of Children Codes, (Measures PCU B1-PCU B7). Part 5 services • Use highly effective age assurance to prevent children from accessing your service, following Ofcom's Guidance on highly effective age assurance for Part 5 services. • Refer to Section 3 and 4 of the Statement on Age Assurance and Children's Access to understand the scope of Part 5 and how you can meet all the requirements of the Part 5 of the OSA.	• Ensure children's personal data is only processed where a valid lawful basis has been identified and where the processing would meet the requirements of fairness. • If your terms of service state that children under a certain age should not be accessing your services, you must ensure that you deploy robust age assurance mechanisms to prevent this from happening and minimise the risk of unlawful processing. • Establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your information processing. Where it is not appropriate for children to access your service, you **should** focus on preventing access. • If the age assurance measure restricts access to child users effectively, the Children's code will not apply but the service **must** comply with DP law.