# 1. Executive summary

Age assurance plays an important role in keeping children, and their personal information, safe online. It describes tools or approaches that help estimate or assess a child's age and therefore allows services to be tailored to their needs or access to be restricted, where required.

Our Children's code is a statutory code of practice. It sets out how internet society services (ISS) likely to be accessed by children should protect children's information rights online. We have withdrawn our opinion published in October 2021 and have replaced it with this updated version. This opinion explains how age assurance can form part of an appropriate and proportionate approach to reducing or eliminating the personal information risks children face online and facilitate conformance with the Children's code.

This opinion is aimed at ISS and age assurance providers to explain how they can use the technology in compliance with data protection law in a risk-based and proportionate way.

**Further reading**

Please see our guidance for further information about services in scope of the code.

## 1.1 What is age assurance?

"Age assurance" refers collectively to approaches used to:

- provide assurance that children are unable to access adult, harmful or otherwise inappropriate content when using ISS; and
- estimate or establish the age of a user so the ISS can be tailored to their needs and protections put in place appropriate to their age.

We use additional terms throughout this opinion that describe different age assurance approaches:

- Age verification is any method designed to verify the exact age of users or confirm that a user is over 18.
- Age estimation is any method designed to estimate the age, or age-range, of a user, often by algorithmic means.
- Parental confirmation involves someone with parental responsibility confirming the age of a child through an online account.
- Self-declaration is a method where a user is asked to state their age, but no further evidence is needed to confirm the veracity of their statement.
- Waterfall techniques are where different age assurance approaches are combined.

## 1.2 Legislative framework

If an ISS is likely to be accessed by a significant number of children, it is in scope of the code and you **should** either:

- establish the age of your users to comply with the code; or
- apply all standards of the code to all users in a risk-based and proportionate way.

If it is not appropriate for children to access your service, you **should** focus on restricting access.

Services may also be subject to other age assurance requirements, for example where they are in scope of the Online Safety Act (OSA). User-to-user services, search engines and services which publish regulated provider pornographic content are all subject to age assurance requirements. If you are a service that is in scope of the OSA and you process personal information, you **must** comply with data protection law.

## 1.3 What are the Commissioner's expectations for age assurance under the Children's code?

The age assurance method you use depends on the risks your personal information processing creates for the child and what level of age certainty is required.

### Manage risk

If your personal information processing activities are likely to present a high risk to children's rights and freedoms, you **should** either:

- apply all relevant code standards to all users to ensure risks to children are mitigated; or
- introduce age assurance methods that give the highest possible level of certainty on users' age.

High risks to children include:

- large scale profiling;
- invisible processing;
- location tracking; and
- using innovative technologies, such as smart devices.

In these circumstances, you **must** complete a data protection impact assessment (DPIA). This helps you assess the data risks to users, particularly children, and explains how you will mitigate these risks.

### Apply the data protection principles

When implementing an age assurance method, you **must** do so in compliance with the data protection principles. You **must:**

- Make sure it is fair.
- Establish a lawful basis to process the information.
- Be transparent about how you use information.
- Not use information collected for the purpose of age assurance for any other incompatible purpose.
- Collect the minimum information required for the process.
- Make sure the method is accurate.

- Not retain any information collected by the method for longer than is needed.
- Make sure the method is secure.
- Be accountable for your compliance with the law (eg by adopting relevant policies and procedures).

## Consider the implications of using AI-driven age assurance methods

There are additional data protection requirements when using artificial intelligence (AI) driven age assurance methods, for example:

- Some AI driven age assurance methods use biometric data. In many cases biometric data will also be special category data. You **must** therefore determine if the processing constitutes special category data as per UK GDPR, which is subject to additional protections.
- Profiling may be used for age assurance (eg by monitoring a users' interests or use of language). You **must** balance the risks that are posed by the use of profiling against its benefits in helping establish the age of your users.
- You **must** address bias and not be discriminatory.
- You **must** make sure that the methods are sufficiently statistically accurate.

The privacy risks children face in the online world can have a significant impact. The potential severity of these risks means that the Commissioner expects you to take the necessary steps to protect children. Age assurance is a crucial component in this, helping you provide an age-appropriate experience, or restrict access to underage users where appropriate. This opinion explains how to do so in a risk-based and proportionate way, whilst respecting users' privacy.

# 2. Introduction

An overarching aim of the Children's code is to ensure that all children are given an age-appropriate level of protection. Age assurance is an important part of the most fundamental standard in the code: considering the best interests of the child.

> "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."

While the code does not mandate the adoption of any one solution, age assurance techniques can play an important role in how you achieve this outcome. For example, age assurance may:

- protect children from harms arising from the processing of their personal information;
- enable you to provide information to children, in a way that is appropriate to their age group, about how you collect, process and use their data; and
- protect children from intrusive activities, such as profiling, marketing and behavioural advertising.

However, you **must** use age assurance carefully as it carries its own types of risk. For example, it:

- may be disproportionately intrusive. For example, some approaches may require access to documentation which can include special category data;
- may introduce risks of inaccuracy. For example, if not implemented effectively some approaches could have a level of accuracy that may result in some young adults being falsely identified as under 18 and denied access to services they are entitled to use. Conversely, an adult may be inaccurately classified as a child and gain access to under 18 only communities;
- may result in exclusion or discrimination of already marginalised groups due to bias, inaccuracy or requirements for official documentation. Those in more disadvantaged socio-economic groups are more likely to lack the documentation they need and be affected by algorithmic bias. Non-white ethnicities and disabled people are over-represented in these groups. People may be unable to use some types of age assurance due to physical or cognitive reasons and risk being excluded from services they are entitled to access; and
- some methods can be circumvented. For example, a child or parent could provide false information in a self-declaration, or a child could log into their parent's account to complete account confirmation.

## 2.1 What is an Opinion and why are we publishing this update now?

Article 58(3)(b) of the UK General Data Protection Regulation (UK GDPR) and section 115(3)(b) of the Data Protection Act 2018 (DPA 2018) allow the Information Commissioner to issue opinions to Parliament, government, other institutions or bodies, as well as the public, on any issue about protecting personal information. The Commissioner can issue opinions on his own initiative or on request.

Stakeholders have sought further information to inform their approach to age assurance, which remains challenging for many organisations. In particular, they have asked for more clarity from the Commissioner on:

- the levels of risk arising from different types of processing and the corresponding level of age certainty required to identify child users and mitigate the risks;
- the level of certainty that various age assurance solutions provide, and confirmation of which providers or types of solutions comply with data protection requirements;
- how to collect the additional personal information required for age assurance while complying with the data minimisation principle;
- how to determine if they are likely to be accessed by children, and therefore fall within scope of the code's age assurance requirements; and
- how other legislative requirements could impact on their need to implement age assurance.

This opinion provides the Commissioner's current view on these issues, including how you can ensure you use age assurance in a data protection compliant way. It is based on existing legislation, standards, guidance and developments at the time of publication. It may inform the Commissioner's approach to regulatory action relating to the code and data protection legislation.

When we published the first version of the opinion in October 2021, we committed to review it as part of the planned, overall review of the Children's code one year after the end of its transition phase. Since we published the first opinion, we have:

- engaged with stakeholders through a call for evidence and focus groups;
- conducted voluntary audits of age assurance providers and ISS to better understand how industry is undertaking age assurance;
- reviewed data protection impact assessments (DPIAs) to understand how ISS identified risks to children, and how decisions were made on what age assurance methods, if any, were used to mitigate those risks;
- undertaken research projects, some jointly with Ofcom, on children's and parents' attitudes to age assurance, and on measures of accuracy for age assurance;
- published guidance for ISS on how to determine if they are likely to be accessed by children;
- reviewed the requirement for an impact assessment in line with our Impact assessment framework and decided that impacts are sufficiently addressed through the Likely to be accessed impact assessment and Children's code impact assessment; and
- engaged with Ofcom to ensure regulatory alignment between the age assurance requirements of the code and the Online Safety Act 2023 (OSA).

The Commissioner reserves the right to make changes or form a different view based on further findings or changes in circumstances. For example, the Commissioner acknowledges that the age assurance market is developing rapidly and will keep these issues under review.

## 2.2 Scope of this opinion

This opinion is aimed at ISS and age assurance providers. It builds on standard 3 of the code. It describes a risk and standards-based approach to age assurance that will help you choose the right solution for your

circumstances.

It will be useful if you seek to use age assurance to conform with the code or prevent high risk data processing being accessed by children. It does not apply to the use of age assurance in physical spaces like retail settings.

This opinion will help you to comply with your obligations under the UK GDPR and wider regulatory frameworks. However, it is not written solely for these circumstances, so you will need to assess the relevance and applicability of this opinion to your circumstances. We are working in co-operation with other regulators to ensure a coherent approach.

## 2.3 How should this opinion be used?

To help you to understand data protection law and good practice as clearly as possible, this opinion says what organisations **must, should** and **could** do to comply.

### Legislative requirements

- **Must** refers to legislative requirements.

### Good practice

- **Should** does not refer to a legislative requirement, but what we expect you to do to comply effectively with the law. You should do this unless there is a good reason not to. If you choose to take a different approach, you must be able to demonstrate that this approach also complies with the law.
- **Could** refers to an option or example that you could consider to help you to comply effectively. There are likely to be various other ways you could comply.

# 3. Age assurance methods

There are four main approaches to age assurance. You can use these individually or in combination. You **should** inform your approach by the risks your data processing creates for children. The following sections describe these methods and their features to help inform your considerations when applying these technologies.

You **should** ensure that any age assurance system you implement has an appropriate level of technical accuracy, reliability and robustness, whilst operating in a fair way to its users, based on the level of risk posed. We intend to produce future guidance for ISS around the accuracy and overall efficacy of different age assurance methods. You **should** also check whether solutions you are considering are certified against recognised industry standards.

Age assurance can also create privacy risks. Article 25 of the UK GDPR explains the need for data protection by design and default. When deciding how to implement age assurance, you **must** consider whether less privacy-intrusive approaches can achieve the same objective.

You **must** consider other legislative requirements to implement age assurance, including your obligations under the OSA.

**Further reading**

Please see our guidance about Data protection by design and default.

## 3.1 Age verification

Age verification is any method designed to verify the exact age of users or confirm that a user is over 18.

There are different approaches to age verification:

- Verifying the user's age through scanning a 'hard identifier' such as a driving license or passport.
- Verifying a person's age through a third-party provider, which can use a range of information sources (eg credit card information, banking information or voter registration records).

You **must** ensure the amount of personal information you collect about a person to verify their age is proportionate to the risks that your service poses.

Age verification does not always require you to collect and store large amounts of personal information. You may be able to verify a user's age without directly collecting their actual age or date of birth. Many third-party providers supply a 'yes or no' response to confirm a user meets the minimum age requirement of a service. Further information on your obligations when using a third party for age verification are outlined in the accountability section.

Verification solutions based on 'hard identifiers' could exclude or indirectly discriminate against people who lack the necessary documents or information, such as credit history or passports. They may pose challenges for children, as they are less likely to possess many of the hard identifiers or options that are

used in these solutions. Where possible, you **should** consider offering a choice of age assurance methods, appropriate to the needs of your service and your users. You **should** consider how to minimise exclusion risks associated with hard identifiers in a way that is appropriate to the risks.

## 3.2 Age estimation

Age estimation is any method designed to estimate the age, or age-range, of a user, often by algorithmic means.

You **could** use age estimation approaches for initial onboarding or account creation, or for ongoing monitoring. These approaches estimate the age of a person, rather than confirming whether someone is a specific age (eg through documentary evidence or a trusted third party). As they do not require documentary evidence, you **could** find this is a more privacy-friendly method than using hard identifiers.

Age estimation systems use a mix of methods, including:

- **A computer vision-based approach** - this estimates age from an image of the person. The image may be captured in real time by a mobile device camera or webcam. Facial age estimation has seen significant progress and is now the most widely used age estimation approach. It has high levels of reported accuracy and efficacy, albeit with variances in relation to skin tone, sex and age.
- **Other biometric approaches** - such as voice analysis to estimate a person's age. This area is continuing to develop, with other biometric approaches launched to market recently and achieving accreditation. Whilst the efficacy of these products is improving, currently they tend not to reach the higher levels of accuracy that would make them appropriate for high-risk scenarios.
- **Analysing account profiling or information** - information derived from the person's activity on the platform. This may include analysing their digital footprint, which looks at their interaction or accounts across many different sites. This may be via a person's email address or mobile phone number, for example. It can also include analysing on-site behaviour once a person is using a service, such as activities, content choices, or friends that suggest the person is below the minimum age of the terms of service. The efficacy of these methods varies.

## 3.3 Self-declaration

Self-declaration is a method where a user states their age but is not required to provide evidence to confirm it. It is a popular approach because there are relatively few steps to follow, and because it requires minimal personal information. It often takes the form of a tick box to self-affirm that the person meets the age requirements in the terms of service.

The OSA states that a method which requires users solely to self-declare their age is not age verification or estimation. This is because it is based entirely on trust and can be easily circumvented and therefore doesn't significantly mitigate risk. You **should** avoid using a self-declaration age assurance method as it is unlikely to be accurate and effective, if:

- there are significant risks to children from the data processing on your site; or
- you are choosing to restrict access to underage users from an adult site.

Self-declaration can be minimally intrusive, and you **could** consider using it for ISS activities which do not

pose a high risk to children, or in conjunction with other methods. It enables you to customise content or processing to the needs of different age groups where there is a low incentive for children to lie about their age.

You **could** increase the effectiveness of self-declaration by applying technical measures. For example:

- preventing people from immediately attempting to re-register if they are denied access on first declaration for being underage; and
- closing the accounts of people discovered to be underage.

However, even if you apply additional technical measures, the process can still be easily circumvented.

You **could** combine self-declaration with techniques that analyse account profiling or information which look for 'red flags' that contradict a person's declared age or age range. Where these indicate that a user is below the minimum age of the terms of service, you **could** then ask the user to confirm their age using an alternative age assurance method.

However, there is a risk that you may be processing the personal information of underage users unlawfully between the initial self-declaration of age and the identification of an underage user. You **should** assess the potential for unlawful processing of children's information in these circumstances. This will identify if there is a risk of harm that you **should** address through an alternative age assurance method.

**Further reading**

Our research on families' attitudes towards age assurance is available here.

## 3.4 Waterfall techniques and age buffers

The waterfall technique combines different age assurance approaches. Waterfall techniques build on the output of successive age assurance approaches to provide a cumulative result with a greater level of confidence than any of these approaches in isolation.

When used correctly, waterfall techniques have the potential to offer high levels of confidence, while providing a privacy respecting approach for users.

A common example is if you combine an age estimation method with a secondary age verification method when you require a high level of assurance.

Some age estimation methods can provide a high level of assurance where the person is clearly over the age threshold. For example, when someone over 40 is looking to access a service for only those over 18 years of age.

The potential for errors may increase for people who are closer to a set threshold (ie the risk of a 16-year-old receiving an estimate they are 18, or a 19-year-old receiving an estimate they are 17).

You could apply an age buffer. This means that a person that is close to the minimum age required to access the service would be required to complete a further age check, using an age verification method.

A use-case scenario for a waterfall technique requiring people to establish they are 18 or over could involve the following:

- An age estimation method is deployed with a buffer of plus seven years.
- All people reported as over 25 pass without further checks.
- All people identified as being under 25 are referred to a secondary age assurance method (ie a choice of credit card check or production of official ID or mobile phone check).

If you choose to use a waterfall technique, you **must** allow people to challenge the decision.

If you are relying on solely automated decision-making, depending on the impact of that decision on the person, there may be additional data protection requirements.

You **must** carefully design waterfall techniques to ensure they achieve increased accuracy whilst preserving privacy. A poorly designed waterfall technique risks collecting unnecessary information which provides little additional assurance. This may result in an unjustified level of privacy intrusion which risks non-compliance with the data minimisation principle.

**Further information**

Further information on rights relating to automated decision making is available here.

## 3.5 Age assurance and conformance with standard 3 of the code

We will take into account the products currently available in the age assurance marketplace when considering whether you have conformed with the age-appropriate application standard of the code. We will continue to monitor and evaluate the activity of the Children's code and associated guidance.

The expectation of "highest possible" certainty on the age of users for high-risk services reflects these commitments. We do not expect you to implement age assurance methods that:

- are not currently technically feasible;
- pose a significant and disproportionate economic impact on businesses; or
- pose risks to the rights and freedoms of people that are disproportionate to the other processing activities on the service.

You **should** be able to demonstrate that you have considered appropriate age assurance options. You **should** also evidence disproportionate costs, disproportionate impacts on people, and technical explanations for why you are not using age assurance methods that may provide higher certainty.

The ecosystem for age assurance standards is continuing to develop. We will take into account adherence to such standards when considering whether you are deploying age assurance methods of an appropriate level of certainty.

**Further reading**

Further information on our regulatory approach is available here.

# 4. Legislative framework

This opinion outlines some of the legislative frameworks about age assurance. It explains your responsibilities under our Children's code. It also sets out considerations when deciding on your approach to age assurance if your service is likely to be accessed by children.

The UK data protection regime is set out in the DPA 2018 and the UK GDPR. It requires you to take a risk-based approach when you use people's personal information, based on principles, rights and obligations. We published the Children's code to help you understand your obligations to ensure you offer online services to children in a way that is compliant with UK data protection law.

We recognise that many providers also have obligations under other legislation, including the OSA. In November 2022, we published a joint statement with Ofcom on online safety and data protection to promote compliance with both regimes.

Ofcom is the regulator for the OSA. It is responsible for implementing the regime and supervising and enforcing the online safety duties. Ofcom will be publishing codes of practice and guidance which will provide more detail about the regime.

The OSA places requirements for age assurance on organisations that fall in scope. These requirements are separate to the Children's code standards. If you are a service that is in scope of the OSA and processing personal information, you **must** comply with data protection law. You **should** also conform with the Children's code if you are a service that is likely to be accessed by children.

## 4.1 Are we in scope of the Children's code?

The code provides guidance on how to comply with the UK GDPR by setting out specific protections you **should** build in when designing online services likely to be accessed by children.

It applies to "relevant information society services which are likely to be accessed by children" in the UK. An information society service is defined as:

> "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."

The code applies to services that are intended for use by children and to services that are not aimed at children but are likely to be accessed by a "significant number of children".

Standard 3 of the code sets out the approach to age-appropriate application. It states that ISS **should**:

> "take a risk-based approach to recognising the age of individual users and ensure you effectively apply

the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead."

If a significant number of children are likely to access your service, you **should** conform with the standards of the code in a risk-based and proportionate way. You **should** use age assurance to conform with the code when:

- your service is likely to be accessed by children and you wish to establish the age of your users as part of your compliance with the code; or
- you provide an adult service and wish to restrict access to children. If restricting access is done effectively so that children no longer represent a significant number of users, the code does not apply.

If it is not appropriate for children to access your service, you **should** focus on preventing access.

**Further reading**

Guidance to help you identify if you are likely to be accessed by children can be found here.

## 4.2 Are we in scope of the Online Safety Act?

The OSA requires that age assurance is applied to the following types of online services where they have links to the UK:

- User-to-user services.
- Search services.
- Services which publish or display regulated provider pornographic content.

The OSA acknowledges the links between the requirements in the Act and data protection legislation. When implementing age assurance, services in scope of the OSA are under a duty to have particular regard to protecting users from a breach of privacy legislation. This includes data protection legislation. This opinion will be a helpful resource to support you with this requirement.

If you are a service in scope of the OSA, you will need to consider applying age verification and age estimation where required by the OSA.

Ofcom will set out more information about the OSA in codes of practice and guidance. You should familiarise yourself with these documents as they become available.

## 4.3 Overview of the application of the legislative framework

All organisations that use personal information are required to comply with UK GDPR and the DPA 2018. The Children's code sets out what ISS in scope of the code **should** do to comply with this legislation when processing children's information. The table below categorises different types of organisations and explains

where standard 3 of the code on age-appropriate application applies, and where the OSA applies.

| Type of organisation | Applicable requirements |
| --- | --- |
| ISS that are likely to be accessed by children, but are not in scope of the online safety regime. | **Children's code**<br>• 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 code to all your users instead. |
| ISS that are likely to be accessed by children and are user-to-user or search services in scope of the OSA. | **Children's code**<br>• 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 code to all your users instead.<br>**OSA**<br>• Services should refer to Ofcom's online safety codes of practice and guidance. |
| ISS that are likely to be accessed by children and are in scope of part 5 of the online safety regime (regulated provider pornographic content). | **Children's code**<br>• 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.<br>**OSA**<br>• Services should refer to Ofcom's online safety codes of practice and guidance. |
| Adult online services that are not likely to be accessed by children, but which deploy age assurance to restrict child access. | **Children's code**<br>• If the age assurance restricts access to child users effectively, the children's code will not apply.<br>**OSA**<br>• Services should refer to Ofcom's online safety codes of practice and guidance. |

# 5. Risk assessment and age assurance

Assessment of risk is a key part of your data protection obligations.

Many data-related risks faced by children are similar to those faced by adults. However, in many cases both the likelihood and severity of harms are greater for children than adults.

Recital 38 of the UK GDPR emphasises that:

> "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing…"

You can use a risk assessment to help determine if it would be suitable to implement an age assurance method.

## 5.1 How the code addresses risk

The protections and safeguards referred to in Recital 38 are explained in the code's standards. Standard 1 states that:

> "The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child."

You **should** use the United Nations Convention of the rights of the child (UNCRC) to identify and assess information-related risks to children. The UNCRC describes children's universal rights and freedoms, which when contravened are likely to harm them.

You **could** use our "Best interests framework" to support you to apply the UNCRC and identify where ISS activities pose risks to children. This looks at the ways that processing of children's information may have a negative impact on each of the rights in the UNCRC. For example:

- the right to life, survival and development (Article 6 of the UNCRC) could be negatively impacted by the use of geolocation data sharing leading to physical harm (eg through stalking);
- the right to development and preservation of identity (Article 8 of the UNCRC) could be negatively impacted by sharing identity information with third parties or profiling that infers characteristics such as ethnicity and gender without adequate protections; and
- the right to protection from economic exploitation (Article 32 of the UNCRC) could be negatively impacted by personalised advertising or sharing of children's information for commercial gain without safeguards.

The code and the best interest's framework only cover risks that arise from processing personal information. Risks to children not related to this type of processing are outside the scope of the code.

Standard 3 of the code on age-appropriate application advises that organisations **should** take a risk-based approach to recognising the age of individual users. You **should** either:

- establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing; or
- apply the standards of the code to all your users.

We have updated our self-assessment risk toolkit which provides practical steps for you to ensure a proportionate and risk-based approach to protecting children's information.

Data protection risks may lead to real harms to people. You must consider the information processing risks to people when you consider what age assurance method(s) to use. Our data protection harms taxonomy can assist you in considering the potential harms which may arise through information processing on your platform.

**Further reading**

Further guidance is available here:

- Children's code self-assessment risk tool.
- Overview of data protection harms and the ICO taxonomy.
- Children's code: best interests framework.
- United Nations Convention of the rights of the child.

## 5.2 ISS activities likely to result in high risk to children

Your services will be considered high risk if:

- the likelihood of harm to children occurring from processing their personal information is high;
- the impact of the harm is not minimal; or
- there is a reasonable possibility of serious harm occurring.

In these circumstances, you **must** complete a data protection impact assessment (DPIA).

You may conclude that the activities are not high risk, or that mitigating measures can reduce the risks. In this case, you **must** document your decisions to show how you have assessed and mitigated these risks.

If you are unable to mitigate any high risks to children, you **must** consult with us prior to starting the processing, in line with Article 36 of the UK GDPR. If you fail to do so, we may see this as an aggravating factor in any regulatory action we take.

We published guidance on data processing activities that are considered "likely to result in high risks". These include:

- large-scale profiling of children (eg to identify children as belonging to particular groups, for automated decision-making, analysing social networks, or to infer interests and behaviours);
- invisible processing of children's information that the ISS did not obtain directly from users (eg list brokering, information sharing with third parties, and online tracking of children);
- targeting children for marketing and advertising (eg personalising marketing content based on children's personal information).
- tracking children – this includes tracking the child's use on the service, or geolocation tracking (eg web and cross-device tracking, fitness or lifestyle monitoring using connected devices and ISS reward schemes);
- processing personal information with risks of physical or developmental harm to children (eg information that reveals children's physical location or health);
- Processing personal information with risks of detrimental use (eg processing which is demonstrably against children's wellbeing, as defined by other regulatory provisions, government advice, or industry codes of practice); and
- processing personal information that involves using innovative technologies (eg artificial intelligence), smart technologies (eg wearables), or some Internet of Things applications which are demonstrably against children's wellbeing.

The code sets standards for information processing to apply where risks to children are likely to be high (eg around profiling and information sharing).

**Further reading**

Further guidance is available here:

- Examples of processing 'likely to result in high risk'.
- Tools for completing a data protection impact assessment (DPIA).
- Children's code: standard 12. Profiling.

## 5.3 High-risk and age assurance certainty

Standard 3 of the code specifies that you **should** either:

- apply all standards of the code to all users; or
- establish the age of your users to a degree of certainty which is appropriate to the risks present on your service.

This ensures that you tailor services and protections to the age profile of your users.

Where services are high-risk, if you choose not to apply the standards of the code to all users, you **should** introduce age assurance methods that give a high level of certainty on the age of users. If your service is deemed inappropriate for children in all circumstances, you **should** focus on restricting access to children.

For high-risk services, you **should** introduce methods with the highest possible level of certainty on the age of users (as opposed to specifying specific appropriate methods). This acknowledges that the certainty will

vary across services. This is due to a range of factors including:

- technical feasibility;
- whether your service is used by authenticated or non-authenticated users; and
- the age range and capabilities of your users.

The Commissioner does not consider that self-declaration on its own is an appropriate method for services that are considered high risk. However, you **could** use self-declaration alongside other age assurance methods where you can demonstrate that the combination is effective.

You **should** be able to demonstrate that you have considered a wide range of age assurance options. You **should** evidence your rationale for choosing a particular method, taking into account the level of certainty the method provides.

## 5.4 Processing children's personal information which doesn't pose a high-risk

Age assurance can also be a helpful tool when your service does not present high risks to children. For example, you **could** introduce the following age assurance methods that process minimal personal information in order to:

- restrict access for child users who don't meet your terms of service;
- identify the age of children to ensure the service you offer is appropriate for their age group; or
- provide privacy and transparency information suitable to the specific age of the child.

Alternatively, you **could** choose to apply the standards of the code to all users in a proportionate way to mitigate any further personal information processing risks you have identified. This is also a privacy-friendly approach that has benefits for all users.

If your service presents minimal information processing risks to children, self-declaration may be appropriate. Where you establish that the risk levels are higher, and you require a higher level of age assurance certainty, you **could** supplement this method with other more accurate age assurance methods. These would provide a higher level of certainty on the age of child users providing this is proportionate to the risks you've identified.

## 5.5 Adult-only sites and age assurance

For services that are age-restricted in law (eg gambling or restricted goods sales), you **should not** be led to the perverse outcome of making your services child-friendly due to the code. If you provide such services, you **should** focus on preventing access by children. We will continue to work with Ofcom and the DRCF to ensure that these broader online safety risks are managed.

The code applies to ISS likely to be accessed by a significant number of children. This includes services not specifically aimed or targeted at children, but nonetheless likely to be accessed by under 18s.

If a significant number of children are accessing your service, there are two options. You **should:**

- apply the principles of the code to all users in a risk-based and proportionate way; or

- if it would not be appropriate for children to access your service, apply age assurance methods appropriate to the data processing risks, restricting access by under 18s so that a significant number are no longer likely to access the service. If access is effectively restricted, the code does not apply.

You may also have duties under other legislation to restrict access to children, including online safety and restrictions on access to gambling services. The OSA places a duty on providers of pornographic content to ensure that children do not encounter pornographic content by using age assurance methods. Section 6 of this opinion provides more details on these requirements.

**Further reading**

Guidance on how to assess whether your service is likely to be accessed by children under the Children's code is available here.

## 5.6 Age-gating

If you use an age-gating page to prevent access to your service to under 18s, it is not within scope of the code if:

- it ensures that children are not accessing the service;
- the methods are robust and effective and therefore prevent under 18s accessing the service; and
- it is not an extension of the adult service (eg. the age-gating page does not allow access to parts of the adult site before age assurance occurs).

Under data protection law, it is unlikely that self-declaration is an effective way to fully restrict access of high risk services to underage users.

You **must** ensure that your age-gating page is compliant with data protection legislation.

# 6. Expectations for age assurance and data protection compliance

This section outlines the main data protection principles and requirements that you **must** take into account in the context of age assurance. If you are implementing age assurance systems, you **must:**

- consider the risks to children that arise from your platform or service;
- determine whether age assurance of users is necessary; and
- select an approach that is appropriate and proportionate to the risk.

You **must** embed data protection into the design of your products, services and applications.

When assessing the age of your users, you are likely to be processing both adults' and children's personal information. Data protection law requires you to protect everyone's personal information. This section therefore applies to the processing for all users when you are assessing their age.

## 6.1 Principles

The UK GDPR sets out seven key principles which lie at the heart of data protection. You **must** follow these when processing personal information. The principles are interlinked, and you may find that complying with one principle helps you to comply with another.

### 6.1.1 Lawfulness

You **must** identify a lawful basis before you start processing personal information for age assurance purposes. There are six lawful bases to choose from. Lawfulness also means not doing anything with the personal information that is unlawful in a more general sense.

The two lawful basis that you are most likely to consider for age assurance processing are legitimate interests or legal obligation.

Legitimate interests involves a three part-test which includes demonstrating necessity and balancing the rights and freedoms of people. It places particular emphasis on the need to protect the interests and fundamental freedoms of children.

Legal obligation applies to processing that you are legally obliged to do. This requires you to demonstrate necessity. For example, it might be appropriate for age assurance required by online safety legislation or gambling licencing conditions.

Some age assurance techniques rely on biometric data which can uniquely identify someone. This is more sensitive personal information, categorised as special category data under UK GDPR and is given additional protections.

**Further reading**

Guidance on the principles is available here: Data protection principles - guidance and resources.

Further guidance on lawful bases is available here:

- What do we need to consider when choosing a basis for processing children's personal data?
- A guide to lawful basis.
- Legitimate interests.
- Legal obligation.
- Special category data.

### 6.1.2 Fairness

If you use people's information for age assurance, you **must** be fair. Fairness means that you **must** only handle it in ways people would reasonably expect and it does not have an unjustified adverse impact on them. You **could** use market research or user testing to help establish what users' reasonable expectations in this context are.

The code requires that you **should not** process children's personal information in ways that are obviously, or have been shown to be, detrimental to their health or wellbeing. To do so would not be fair.

Fairness in data protection law is broader than fair treatment and non-discrimination. When using age assurance, you **should** scrutinise and minimise any potential bias in your approach.

You **must** provide tools so that people can challenge inaccurate age assurance decisions. You **should** make these tools accessible and prominent, so people can exercise their rights easily.

Where you determine age through solely automated decision-making, Article 22 of the UK GDPR has additional rules to protect people and ensure that processing is fair.

**Further reading**

Further guidance is available here:

- Principle (a): Lawfulness, fairness and transparency.
- Children's code standard 15 – online tools.
- What is the impact of Article 22 of the UK GDPR on fairness?

### 6.1.3 Transparency

Transparency is fundamentally linked to fairness. If you are not clear and transparent about how you will process people's information for age assurance, it is unlikely that your processing will be fair.

People have the right to be informed about your processing of their personal information. You **must** be clear, open and honest about how you use people's information for age assurance purposes, and how you make decisions.

Standard 4 of the code provides advice on how you **should** present this type of information to children.

You **should** consider how age assurance fits into your user journey and experience to determine how and when it is best to provide this type of information.

Regardless of the method used for age assurance, you **must** explain clearly to people:

- why you are using age assurance;
- what personal information you need for the age assurance check;
- whether you will use a third party to carry out the age assurance check;
- how you use the personal information and how it will affect the user's experience of the platform or service;
- whether you keep personal information you collect for age assurance and how, why and for how long; and
- the rights available to people, including how they can challenge an incorrect age assurance decision.

You **must** be able to explain how you arrived at the decision, in a way that people can understand.

If you are relying on solely automated decision-making, depending on the impact of that decision on the person, there may be additional data protection requirements.

People have the right to be informed. Children have the same rights as adults, including the right to rectification and the right to be forgotten. Even if a child is too young to understand the implications of their rights, they are still their rights rather than anyone else's, such as a parent or guardian. In Scotland there is a presumption that a child of 12 or over has sufficient understanding to be able to exercise their rights. There is no equivalent presumption elsewhere in the UK.

You **should** only allow parents to exercise these rights on behalf of a child if:

- the child authorises them to do so;
- the child does not have sufficient understanding to exercise the rights themselves; or
- it is evident that this is in the best interests of the child.

**Further reading**

Further guidance is available here:

- Children's code standard 4 – Transparency
- What rights do children have?
- Rights related to automated decision making including profiling

### 6.1.4 Purpose limitation

You **must** only process personal information for specific and legitimate purposes, and not further process it in a manner incompatible with those purposes. Purpose limitation is closely linked to transparency, fairness, and data protection by design.

If you are implementing an age assurance system, you **must:**

- be clear about what personal information you process;
- be clear about why you want to process it;
- ensure you only collect the minimum amount of personal information you need to establish an appropriate level of certainty about the age of your users; and
- ensure you do not use personal information collected for age assurance for any other purpose, unless the new purpose is compatible with age assurance.

If you are a developer of age assurance systems, you **must** build your systems with data protection in mind.

You **must not** re-use personal information collected for age assurance for purposes such as profiling for advertising, or in other ways that are incompatible with the purposes you collected it for.

Information that you have collected during your normal course of providing a service may be relevant for age assurance purposes. You may re-use this information to assess someone's age, but only if:

- the age assurance process is compatible with your original purpose for collecting information;
- you have the appropriate level of consent; or
- you have a clear obligation or function set out in law.

You **must** ensure that the new use of personal information is fair, lawful and transparent.

Purpose limitation also applies to sharing personal information. Standard 9 of the code notes that you **should not** share children's information, such as children's age assurance information, unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child. Where you have to share children's age assurance information, you **should** demonstrate and document why it is necessary to do so. In your privacy notice, you **must** clearly state circumstances when you might need to share this information.

**Further reading**

Further guidance is available here:

- Principle (b): Purpose limitation.
- A 10 step guide to sharing information to safeguard children.
- Children's code standard 9 - Data sharing.
- Children's code standard 12 – Profiling.

### 6.1.5 Data minimisation

You **must** ensure that the personal information you collect is adequate, relevant and limited to what is necessary for the purpose.

Age assurance may require you to process personal information beyond what is involved in delivering your core service. You **must** apply data minimisation to your chosen age assurance approach. This means that you must make sure that the personal information you process for age assurance purposes:

- is sufficient to properly achieve the stated purpose of the age assurance (adequate);
- has a rational link to that purpose (relevant); and
- is no more than you need for that purpose (limited to what is necessary).

The data minimisation principle means that the personal information you collect **must** be adequate to achieve your purpose. In the context of age assurance, self-declaration can be easily circumvented, which means the information you collect is likely to be insufficient for high-risk scenarios. Therefore, you may require more personal information to achieve your purpose. In most cases, as long as you limit your processing to what is necessary and proportionate, it is likely to be appropriate to use age assurance to reduce the risk of harm to children while complying with data minimisation.

You **must** only use personal information necessary to undertake age assurance. What is necessary is linked to what is proportionate for the circumstances. A service or platform that does not pose a high risk to children is likely to need to process less information to assess or verify the age of users than one that poses a high risk to children.

In many cases it may be excessive to see an official document (eg a passport or driving licence). This is because you can use an age assurance method that processes less personal information whilst still being proportionate to the risks faced by children. You may only need to record a yes or no output that a person meets the age threshold.

**Further reading**

Please see our guidance on data minimisation for further information.

### 6.1.6 Accuracy

This section refers to accuracy in the context of data protection, however section 6.3.4 refers to the statistical accuracy of algorithms.

You **must** ensure that the personal information you process for the purpose is accurate.

The accuracy principle applies to all personal information, whether it is about a person used as an input or output to an AI system. This does not mean that an AI system needs to be 100% statistically accurate to comply with the accuracy principle.

You **must** have methods in place to mitigate the risks that the personal information you collect may be inaccurate. When using age estimation methods, you **should** record age assurance returns as an estimation rather than a matter of fact. People have the right to correct inaccuracies in their information which means you **must** consider any challenges to the accuracy.

If you are developing age assurance solutions, you **should** test them for accuracy. If you are using an external solution, you **should** seek evidence from your suppliers, such as certification.

Incorrect outcomes for age assurance are likely to be:

- an adult wrongly identified as a child, or a child wrongly identified as younger than they are, is denied access to a platform or service that is suitable for them to access;

- a child who is wrongly identified as an adult or older than they are, is able to access a product or service that is restricted to adults or children of an older age; or
- an adult wrongly identified as a child gains access to child-only services with a maximum age limit which may result in risks to the child users.

Inaccuracy presents risks. For example, a child who is attributed an incorrect age may access services intended for adults or older children. They may unwittingly consent to further processing of their personal information that leads to inappropriate profiling. In that situation, it is unlawful to process information of children under 13 if there is no evidence of consent from someone with parental responsibility. This is because only children aged 13 or over are able to provide their own consent in these circumstances. Conversely, adults may suffer detriment or harm if they are denied access to services they need.

No system is fool proof. You **should** consider how likely it is that age checks may be bypassed or spoofed (how a system might be deceived into thinking an individual is a different age) and the associated impact. For example, the potential harms which can happen if inaccurate age information is collected about your users. For any age assurance approach, you **should** also consider:

- how an adult or older child wrongly denied access to part or all of a platform or service can challenge a decision;
- how a child wrongly identified as an adult or older than they are (or someone with parental responsibility), can rectify this outcome; and
- whether the potential harm to children accessing an inappropriate platform or service is sufficient to justify ongoing monitoring of all users. For example, to identify children that may have wrongly gained access.

In addition, you **should** consider whether further checks are required when a child reaches age 13 (the age at which they are able to provide their own consent as outlined in Article 8 UK GDPR) and 18 (the point at which they are recognised as an adult). This will ensure that users on the service are only able to access parts of the service which are appropriate to them.

**Further reading**

Please see our guidance on accuracy and the right to rectification for further information.

### 6.1.7 Storage limitation

You **must not** keep people's information for longer than you need it. You **should** be able to justify how long you keep personal information collected for age assurance purposes and you **should** have a policy that sets out retention periods.

You **should** be proportionate in how frequently you carry out age checks compared to the risks on your service. It may be necessary to implement age checks at suitable intervals to ensure the personal information you collect remains accurate. In this case, you **should** erase personal information which you have obtained through previous checks that is no longer required. This ensures that you do not hold age assurance information for longer than necessary.

You **must** retain only the minimum amount of personal information necessary for the purpose. If you use a hard identifier to assess age, you may only need to retain a yes or no output once you've completed the check.

People have the right to have their information erased in certain circumstances. You **must** consider challenges to your retention of personal information you collected for age assurance.

**Further reading**

Please refer to our guidance on the right to erasure and Principle (e): Storage Limitation for further information.

### 6.1.8 Integrity and confidentiality (security)

You **must** process people's information securely when you use it for age assurance purposes. You **must** consider how the system collects or shares information, as well as the personal information involved. You should include this as part of your data protection by design approach and address considerations about risk analysis, organisational policies, and physical and technical measures.

You **must** consider the state of the art and costs of implementation when deciding which security methods to use. You **must** put in place methods that are appropriate both to the circumstances and the risk the processing poses.

If you use a third-party supplier, you **must** ensure appropriate data security methods are in place through due diligence checks.

If using AI, you **should** consider the balance between transparency and security. For example, you **should** ensure that a malicious actor cannot re-identify people given sufficient technical information.

**Further reading**

Please see our guidance on AI and security for further information.

Our general guidance on Principle (f): Integrity and confidentiality (security) is available here.

### 6.1.9 Accountability

The accountability principle means that you **must** be able to demonstrate how your age assurance activities comply with data protection law.

There are a number of accountability measures that you **must** take (where applicable), including:

- adopt and implement data protection policies;
- take a data protection by design and default approach to age assurance;
- put written contracts in place with third party age assurance services that process information on your behalf (these may be processors or joint controllers depending on the exact circumstances of

the relationship);

- maintain documentation of your age assurance processing activities;
- implement appropriate security measures for your age assurance processing; and
- record and, where necessary, report personal data breaches.

You **must** take a data protection by design approach to age assurance. You **must** put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard people's rights. This means integrating data protection into your age assurance activities from the design stage right through the lifecycle.

You **must** be able to demonstrate that your approach to age assurance is proportionate to the risks to children associated with a platform or service.

A DPIA is a key accountability tool that you **must** implement if your processing is **likely to result in a high risk** to people's rights and freedoms. You **should** carry out a DPIA at an early stage in the design of any product or service that involves processing personal information (even if it is not a requirement). This applies for age assurance. Standard 2 of the code explains how DPIAs fit into the wider context of the children's code.

In some cases, age assurance may be unnecessary. For example:

- where you demonstrate that the risks to children are not high;
- where the service is unlikely to be accessed by a significant number of children; or
- if all the content or services you provide to all your users conform to the code.

You **should** assess whether a significant number of children are likely to access your service. You **should** consider this in your DPIA to justify which age assurance method to apply, if any. This helps demonstrate compliance with accountability requirements.

**Further reading**

Further guidance is available here:

- Accountability and governance.
- Controllers and processors.
- Children's code – standard 2 data protection impact assessments.
- 'Likely to be accessed' by children – FAQs, list of factors and case studies.

## 6.2 ICO certification schemes

You **could** use the ICO's approved and published certification schemes to demonstrate accountability. Certification provides a framework for you to follow, helping ensure compliance and offering assurance that specific standards are met.

Certification allows people to assess the data protection compliance of an organisation's age assurance

product, process or service. This provides transparency both for people and in business-to-business relationships.

Applying for certification is voluntary. However, if there is an approved certification scheme that covers your processing activity, you **could** consider working towards it as a way of demonstrating compliance with the UK GDPR.

For example, in 2021 we approved and published the Age check certification scheme (ACCS) which tests that age assurance products work. The scheme includes data protection criteria (ACCS 2:2021) for those organisations operating or using age assurance products.

If you use age verification systems that are not certified, you **should** still be able to provide other evidence that the checks you use are effective.

## 6.3 Age assurance and AI

Artificial Intelligence (AI) has become a standard industry term for a range of technologies. In this section, we outline a number of data protection considerations that may arise when you implement age assurance methods.

### 6.3.1 Biometric data

Age assurance methods may use biometric data, depending on the type of technology deployed.

Some age verification approaches may use biometric recognition technologies to match an image of someone to the photograph on their official documentation to prove their age (eg a passport or a driver's license).

Some age estimation approaches may use biometrics for face or voice analysis and classification to provide an estimate of a person's age.

Both recognition and classification approaches use AI or machine learning (ML). However, from a data protection compliance perspective, the information they process, and the associated obligations on organisations, may differ.

Biometric recognition technologies process biometric data for the purpose of unique identification. In an age verification scenario, an image of the person requesting verification is captured and turned into a biometric template. This template is then compared with another, generated from the image on the official photo ID.

The purpose of the comparison is to find a match between the two images (recognise the person). This means that the age verification solution can be confident that the person presenting is the same person pictured on the official ID. This provides proof (verification) of the person's age (or that their age is over a set threshold). Whenever you use biometric data for the purpose of uniquely identifying someone, it is special category biometric data. Special category data requires further protection due to its sensitive nature.

Before processing special category biometric data, or if the solution you are using is AI-driven, you **must** complete a DPIA. This documents your purpose for processing this information, and assesses and

manages any risks which may arise.

To process special category biometric data, you **must** identify a valid Article 9 condition for processing.

Assuming it is proportionate for your service to use biometric data for age assurance, then it is likely that you can apply the condition for substantial public interest. This is because the processing is likely to be necessary to safeguard children and people at risk (Article 9(2)(g) schedule 1, paragraph, 18 of the DPA).

**Further reading**

Please see our guidance on special category data and biometric data for further information.

### 6.3.2 Age assurance and profiling

Profiling refers to any form of automated processing of information that is used to evaluate or predict someone's behaviour or characteristics. Profiling can involve the use of AI and ML techniques to either inform decision-making or make decisions automatically. AI-based profiling can make inferences about people by making predictions based on patterns that an AI model observes. These systems can classify people into different groups or sectors. This analysis identifies links between different behaviours and characteristics to create profiles of people.

Profiling can be used for age assurance, for example, through monitoring aspects of a user's vocabulary and interests to identify potentially under-age users. You can also use profiling as an age estimation method in itself. However, you **must** consider the confidence you can have in the age inferences gathered, and the fairness and accuracy of any AI system you use to make them. You **must** show that it is proportionate to the risks to children that it is being used to mitigate.

Profiling data gathered for age assurance **must not** be used for any incompatible purpose. If profiling for age assurance relies on cookies, such cookies are permissible under the "strictly necessary" exemption found in the Privacy and Electronic Communications Regulations 2003 (PECR). Your use of profiling **must** be transparent, and you **should** make sure it is within a person's reasonable expectations.

**Further reading**

Please see our guidance on automated decision making and profiling.

Further information about cookies and similar technologies is available here.

### 6.3.3 Age assurance and discrimination

Age assurance may produce discriminatory outcomes. The risk of discrimination may be heightened for people with protected characteristics, such as age, race and disability in a way that would impact the fairness of the processing. If you fail to address bias, you may breach the fairness principle.

Age verification usually depends on the user having ready access to official documents or a credit history. Young adults and people from disadvantaged backgrounds (in which disabled people or those from ethnic minority backgrounds are over-represented) may have lower rates of access to a driver's licence or passport, and so be unable to access an ISS using only age verification.

Age estimation may carry risks from algorithmic bias. Systems based on biometrics, such as voice or facial structure, may not perform as well for people of darker skin tones, or those with medical conditions or disabilities that affect physical appearance. These systems may have discrimination and bias risks. Age estimation technology is advancing rapidly, allowing some providers to significantly reduce the bias in their systems. You **must** review the efficacy and accuracy rates when planning to use age assurance.

Discriminatory outcomes may also be in breach of both the Equality Act 2010, the applicable equality legislation in Northern Ireland and UK GDPR, since processing with discriminatory outcomes is unlikely to be fair. You **must** consider these risks. You **must** ensure that your age assurance solution incorporates reasonable adjustments for disabled people, such as offering alternative methods for age assurance. You **should** have an accessible process for users to challenge an incorrect age assurance decision.

**Further reading**

Please see our guidance about fairness, bias and discrimination for further information.

### 6.3.4 Statistical accuracy

In general, the output of AI processing amounts to a statistically informed guess rather than a confirmed fact. In age estimation solutions, an algorithm provides an estimate of age within a range. While in an age verification solution, an algorithm may make a decision that links someone to an official source that verifies their age. It is important to remember that no algorithm is 100% statistically accurate all the time.

You **must** ensure that any age assurance system is sufficiently statistically accurate and avoids unjust discrimination. You **should** decide and document what your minimum success criteria are for statistical accuracy at the initial business requirements and design phase. Different age assurance methods perform with varying levels of statistical accuracy for different age groups. These due diligence measures include systems provided or operated by third parties.

You **should** test your AI system against these criteria at each stage of the lifecycle. This includes post-deployment monitoring, including for emergent bias.

You may require trade-offs in the design of the AI system. To use a simplified example, there is a balance between precision ("how sure we are that someone has been correctly classified as under 18") and recall ("how sure we are that we have identified all of the under 18s trying to use a platform or service"). Increasing precision means a greater risk of missing some underage users, whereas increasing recall means more adults will be wrongly classified as underage. The correct balance depends on the circumstances, risks and harms you identify.

**Further reading**

Further information is available here:

- What do we need to know about accuracy and statistical accuracy?
- What about fairness, bias and discrimination?
- Annex A: Fairness in the AI lifecycle.

### 6.3.5 Algorithmic fairness

Algorithmic fairness is a term for a range of techniques that can address the risks of an AI model treating people in way that could be discriminatory.

An AI system is only as good as the information used to train or tune it. There are numerous real-world examples where discriminatory outcomes result from algorithms that are trained on information that does not properly represent the population they will be applied to. Usually, the worst effects of such discrimination fall on groups who are already marginalised or at greater risk of harm.

We have said in our AI guidance that AI systems are less accurate for outliers, as by definition they represent a minority in the training data, making them more vulnerable to risks. When choosing an AI system, you **should** ensure that algorithms are trained using high-quality, diverse and relevant data sets. Our guidance on AI and data protection sets out ways in which developers can mitigate biased, discriminatory, or otherwise unfair outcomes resulting from automated decision-making.

You **should** consider capture bias. This is where the device that observes information does so inaccurately. For example, a camera used in poor lighting conditions may produce a photograph of the user that is not of good enough quality for accurate age estimation.

You **should** consider what kind of algorithmic fairness measures would be appropriate for your chosen system. While a statistical approach to fairness can be helpful in identifying discriminatory impacts, it will only address some of the issues you **must** consider to comply with the fairness principle. This is because the concept of data protection fairness covers issues beyond statistical accuracy.

**Further reading**

Further guidance is available here:

- Annex A: Fairness in the AI lifecycle.
- What about fairness, bias and discrimination?
- Automated decision-making and profiling.
- Principle (a): Lawfulness, fairness and transparency.

# 7. Conclusion and next steps

Parliament has acted to implement laws that transform the way we safeguard children when they access online services, via data protection and online safety legislation. Privacy risks are relevant to all users, but the privacy risks that children face in the online world can have a significant impact. Age assurance is an important tool to manage these risks.

The potential severity of these risks means that the Commissioner expects you to take the necessary steps to protect children. Age assurance is a crucial component in this, helping you to provide an age-appropriate experience, or to restrict access to underage users where appropriate.

## Key recommendations for age assurance

You **must** ensure that your age assurance methods comply with data protection law, meaning that you **must:**

- assess the data protection risks of the age assurance method(s) you implement;
- base it on good data protection practices, particularly transparency, fairness, lawfulness, accuracy, data minimisation and purpose limitation;
- clearly explain to child users, in an age-appropriate way how their personal information will be used;
- be able to demonstrate that the approach you use complies with data protection law; and
- ensure your approach is compliant with other legislative requirements, including the OSA and the Equality Act 2010.

## 7.1 Next steps

We will continue to work with stakeholders in the UK and internationally to understand and interpret the legal, technical, and social issues that impact the use of age assurance for online services likely to be accessed by children.

Our work with Ofcom is ongoing, building a coherent approach to our respective regulatory remits outlined in our joint statement.

We will continue our engagement on international standards on age assurance technologies currently being developed by the International Organisation for Standardisation and IEEE (ISO/IEC 27566 and P2089.1). These standards will provide further clarity on technical expectations and processes when implementing a system for use.

The Commissioner intends to replace this opinion with guidance on age assurance in due course. This may include updates on any material legal, technical, or practical developments in this evolving area. He will review the opinion to ensure it is consistent with any changes to data protection law.