Guidance on highly effective age assurance and other Part 5 duties

For Part 5 services

Guidance

Published 16 January 2025

Cntents

Section

Annex

1. Overview

What this guidance covers

This is our statutory guidance produced under section 82 of the Online Safety Act 2023 to assist providers of internet services, who display or publish pornographic content on those services, in complying with their regulatory duties set out in section 81 under Part 5 of that Act. The main duty on these service providers is to ensure, by the use of age verification or age estimation (or both), that children are not normally able to encounter such pornographic content. We use the term **'age assurance'** in this guidance to refer to such verification and estimation.

This document gives guidance on the matters referred to in section 82, particularly:

- matters relevant to assessing whether a service is in scope of the Part 5 duties;
- examples of kinds of age assurance that may be suitable for the purposes of compliance, and criteria that service providers should fulfil to ensure the age assurance implemented is highly effective at correctly determining whether or not a particular user is a child;
- matters relevant to how service providers can keep a written record and produce a publicly available statement setting out how they have complied with these additional Part 5 duties, including how providers may have regard to the importance of protecting users from breaches of privacy law in their written record; and
- the principles that we will normally apply when determining whether a service provider has complied with its duties and where we are likely to consider that it has not complied.

We summarise below the Part 5 duties, together with our recommended key steps to support compliance with those duties as covered in this guidance.

Summary of the Part 5 duties

- Implement age assurance, for example by using one or more of the methods listed in Section 4 of this guidance;
- Ensure that the age assurance process is:
  - of a kind that could be highly effective at correctly determining whether or not a user is a child; and
  - used in such a way that it is highly effective at correctly determining whether or not a user is a child (for example, by considering the criteria set out in Section 4 of this guidance).

- Ensure that, by using the age assurance process in question, children are not normally able to encounter regulated provider pornographic content on the service (i.e., by using an effective **access control** measure)[1];
- Keep an easily understandable written record of:
    - the kinds of age assurance used and how they are used by the service provider or a third-party age assurance provider;
    - how the service provider has had regard to privacy and data protection laws when deciding which age assurance process to use and how.
- Produce a publicly available summary of the parts of the written record relating to implementing highly effective age assurance, including the age assurance method(s) the service provider is using and how it is being used.

Key steps to support compliance with Part 5 duties

- Ensure the age assurance process fulfils the four criteria of technical accuracy, robustness, reliability and fairness;
- Consider the principles of accessibility and interoperability when implementing age assurance;
- Implement any techniques to mitigate against attempts at circumvention of the age assurance process that are easily accessible to children and where it is reasonable to assume that children may use them;
- Consider whether to offer alternative methods where an age assurance method is only highly effective for a limited number of users;
- Ensure that the written record is durable, accessible, easy to understand, and up-to-date;
- Familiarise themselves with data protection legislation, and how to apply it to their age assurance method(s), by consulting guidance from the Information Commissioner's Office ("ICO"); and
- Refrain from hosting, sharing or permitting content that directs or encourages child users to circumvent the age assurance process or access controls.

[1] We use the term "access control" to describe a technical mechanism(s) which prevents users who have not been age assured, or having been age assured, did not meet the requirements of the age assurance process, from accessing a service (or part of it) or certain content.

2. Introduction

Background to the guidance

2.1 The Online Safety Act 2023 ("the Act") creates a new regulatory framework with the general objective of making regulated internet services safer for users in the United Kingdom (UK), particularly for children.

2.2 As part of achieving that objective, section 81 in Part 5 of the Act imposes specific duties on certain providers of such internet services that display or publish regulated provider pornographic content to ensure, by the use of age verification or age estimation (or both), that children are not normally able to encounter such content (the **"Part 5 duties"**). We use the term **'age assurance'** in this guidance to refer to such age verification and age estimation.

2.3 Importantly, section 81 imposes a duty to ensure that age assurance in this context is of a kind and used in a way that is '**highly effective'** at correctly determining whether or not a user is a child.

2.4 The Part 5 duties are imposed on providers of such '**internet services'**[2] as are described in section 80(2) of the Act. We refer in this guidance to providers of such internet services as **'service providers'** and the services within scope of Part 5 of the Act as **'regulated services'**.

2.5 This guidance is produced under section 82 of the Act to assist service providers in complying with their Part 5 duties.[3]

2.6 Service providers are required to comply with their Part 5 duties from 17 January 2025.

2.7 Annex 1 to this guidance contains a glossary of other terms used in this guidance.

Navigating the guidance

2.8 Below, we set out below an overview of each section of this guidance.

Section 3: The scope of the Part 5 duties

2.9 Section 3 provides guidance to service providers as to how they can assess whether their internet services fall in scope of Part 5 of the Act. This includes guidance on:

[2] Section 228 of the Act explains that an 'internet service' means a service that is made available by means of the internet, and that a service is "made available by means of the internet" even where it is made available by means of a combination of the internet and an electronic communications service (within the meaning given by section 32(2) of the Communications Act 2003).

[3] Ofcom has a duty under section 82 of the Act to provide guidance for service providers to assist them in complying with their duties set out in Part 5 of the Act. The Act requires Ofcom's guidance to include several elements, including examples of kinds and uses of age verification and age estimation that are, or are not, highly effective at correctly determining whether or not a particular user is a child, and examples of circumstances in which Ofcom is likely to consider that a provider has not complied with its duties.

- assessing whether content is pornographic content which is regulated under Part 5 (referred to as **"regulated provider pornographic content"**);
- exemptions to Part 5 under the Act; and
- assessing whether a service has links to the UK.

Section 4: The age assurance duties

2.10 Section 4 provides guidance to service providers on how to use age assurance to ensure that children are not normally able to encounter regulated provider pornographic content on their regulated services. This includes:

- a non-exhaustive list of age assurance methods that we consider are capable of being highly effective at correctly determining whether or not a user is a child, and those that we consider are not capable of being highly effective;
- criteria the age assurance process should fulfil to ensure that it is highly effective at correctly determining whether or not a user is a child, and guidance on how to fulfil these criteria;
- principles that service providers should consider to ensure that the age assurance process is easy to use and that, as far as possible, adult users are not unduly prevented from accessing legal content; and
- examples of circumstances where we are likely to consider a provider has not complied with these duties.

Section 5: The record-keeping duties

2.11 Section 5 provides guidance to service providers on the duties relating to record-keeping. This includes guidance on:

- how to keep a written record;
- the content which must be included in the service provider's written records and what must be summarised in a publicly available statement;
- how service providers can have regard to protecting users' privacy; and
- circumstances where we are likely to consider a provider has not complied with its duties.

Section 6: Our approach to assessing compliance with the age assurance and record-keeping duties

2.12 Section 6 provides an explanation of the approach we will take to assessing compliance with the Part 5 duties. This includes:

- our general approach to enforcement of the Act; and
- the principles that we will apply when determining whether a service provider has complied with each of its Part 5 duties.

3. The scope of the Part 5 duties

Internet services subject to the Part 5 duties

3.1 We have already explained the broad meaning of an 'internet service' in section 2 of this guidance. However, section 80(2) applies to specific internet services which meet the following three conditions:

- regulated provider pornographic content is published or displayed on the service ("condition 1");
- the service is not out of scope of Part 5 or exempt ("condition 2"); and
- the service has links to the UK ("condition 3").

3.2 Condition 1 relates to the **type of content** which is published or displayed on the service. Condition 2 relates to the **types of service** which are out of scope of Part 5 or exempt, including on-demand programme services. Condition 3 relates to the intended or actual **user base of the service**.

3.3 This section provides an overview of each of these conditions which determine whether a regulated service is in scope, with reference to the relevant statutory definitions. We also provide some high-level examples to assist service providers in understanding how these definitions apply.

Condition 1: Regulated provider pornographic content is "published or displayed" on the service

What pornographic content falls within Part 5?

3.4 The Part 5 duties relating to age assurance only apply to a specific kind of pornographic content called '**regulated provider pornographic content**' (as defined in section 79(3) of the Act). In that regard, it is necessary to consider whether the content in question falls within the meaning of the Act's definition of 'pornographic content' and, if so, whether it is published or displayed on the service by the provider of the service, or by a person acting on behalf of the provider.

3.5 Pornographic content is defined in the Act as "content of such a nature that it is reasonable to assume that it was produced solely or principally for the purpose of sexual arousal."[4]

3.6 Pornographic content may include artificial images, such as AI generated or animated images.

3.7 Pornographic content might include content which would fall under the British Board of Film Classification's (BBFC) R18 category, which is "primarily for explicit works of consenting

[4] Section 236(1) of the Act.

sex or strong fetish material involving adults."[5] However, other content of a strong sexual nature that seeks to sexually arouse or stimulate, that would not fall in scope of this classification, may also be treated as pornographic.

3.8 Where pornographic content appears online, it will fall within the scope of Part 5 as regulated provider pornographic content if:

- the content meets the definition for '**provider pornographic content'**, meaning it is published or displayed on an internet service by the provider of the service or a person acting on their behalf (as set out in section 79(2) of the Act); and,
- the content is not a category of pornographic content explicitly carved out from that definition; or
- the content is not otherwise exempted or excluded.

3.9 The definition for regulated provider pornographic content includes pornographic content published or displayed on the service by means of:

- a software or an automated tool or algorithm applied by the provider or a person acting on behalf of the provider; or
- an automated tool or algorithm made available on the service by the provider or a person on behalf of the provider.[6]

3.10 The definition of regulated provider pornographic content encompasses content in a range of forms, including still and moving images, audio and audio-visual content. This might include, for instance, a video or explicit photos of sexual activity.

What pornographic content falls outside of Part 5?

3.11 Not all pornographic content is included under the definition of regulated provider pornographic content. The following content is expressly excluded:

- Pornographic content that is user-generated content in relation to an internet service;[7]
- Pornographic content that:

a) consists only of text, or
b) consists only of text accompanied by:

i) a GIF which is not itself pornographic content;
ii) an emoji or other symbol; or
iii) a combination of a GIF which is not itself pornographic content and an emoji or other symbol;[8]

[5] R18 is a special classification, which can only be shown to adults in specially licensed cinemas and can only be supplied to adults in licensed sex shops. BBFC, R18 rating.
[6] See section 79(2)(a) and (b) of the Act.
[7] Section 79(7) of the Act. For a definition of 'user-generated content' see section 55(3) and (4) of the Act.
[8] Section 79(4) of the Act.

- Content that consists of a paid-for advertisement.[9]

3.12 Part 3 of the Act sets out obligations for user-to-user (U2U) services, including the requirement for regulated U2U services that allow pornographic content on their service to use highly effective age assurance to prevent children from encountering it.[10]

3.13 Provider pornographic content may be present on different types of online service, including those which are predominantly U2U services. Such services will be subject to the Part 5 duties in relation to the pornography that the provider itself (or a person acting on behalf of the provider) publishes or displays on the service.

What does "published or displayed by the provider on its internet service" mean?

3.14 As explained above, the Part 5 duties apply where pornographic content is published or displayed by a provider of an internet service or by a person acting on behalf of the provider. For the purposes of Part 5 of the Act, the provider of the internet service will be the entity or individual that has control over which content is published or displayed on the internet service.[11, 12]

3.15 We are likely to consider a service provider to have exercised control over the pornographic content appearing on its service where it exercises editorial control over the nature, selection or presentation of the content. Examples of situations where we might consider pornographic content being displayed or published by the provider of an internet service (be that a natural person or an entity such as a studio) include:

- where an individual who creates pornographic content uploads and publishes it on an online service that they control or run;
- where a studio produces pornographic content and then publishes this content on an online service that the studio controls or runs;

---

[9] Section 79(5) of the Act. An advertisement is a 'paid-for advertisement' in relation to an internet service if -
a) the provider of the service receives any consideration (monetary or non-monetary) for the advertisement (whether directly from the advertiser or indirectly from another person), and
b) the placement of the advertisement is determined by system or processes that are agreed between the parties entering into the contract relating to the advertisement. See section 236(1) of the Act.

[10] See section 12 of the Act. All regulated user-to-user services that are likely to be accessed by children must use highly effective age assurance to prevent children from encountering primary priority content that is harmful to children, including pornographic content (under section 61(2)), except where such content is prohibited on the service for all users.

[11] Section 226(8) of the Act. Section 226(9) also clarifies that, if no entity has control over which content is published or displayed on such an internet service, but an individual or individuals have control over which content is published or displayed, the provider of the service is to be treated as being that individual or those individuals.

[12] Different definitions apply to determine the provider of a user-to-user service or a search service. In the case of a user-to-user service, the provider is the entity or individual with control over who can use the site (section 226(2) and (3) of the Act); in the case of a search service, the provider is the entity or individual which has control over the operations of the search engine (see section 226(3) and (4) of the Act).

- where a service provider has designed and provided interactive games featuring pornographic imagery on an online service which it controls or runs.

3.16 There may be instances where online services include some pornographic content which falls in scope of Part 3 and some pornographic content which falls in scope of Part 5. For example, while tube sites are often U2U services that are predominantly comprised of user-generated pornographic content, a provider of a tube site may itself make some pornographic content available on that site.[13] Where a provider of such a service publishes or displays pornographic content on, for example, a premium sub-section of its site, or someone else does so on its behalf, that pornographic content will be within scope of the Part 5 duties (unless otherwise exempt, for instance if that part of the service is an on-demand programme service, as explained in paragraph 3.26).

Pornography in search results

3.17 Pornographic content which appears in the search results of a search engine or a combined service is not treated as published or displayed on the search service or combined service in question for the purposes of Part 5 of the Act.[14] These services will be subject to obligations in Part 3 of the Act, including the children's risk assessment and safety duties in sections 28 to 30 of the Act (and for a combined service also in sections 11 to 13 of the Act).

Specific circumstances where content is considered "published or displayed on a service"

3.18 The Act specifies some of the circumstances where 'pornographic content' should be considered as "published or displayed on a service", namely:

- content that is only visible or audible to users as a result of interacting with content that is blurred, distorted or obscured (for example, by clicking on the content) but only where the pornographic content is present on the service;
- content that is embedded on the service; and
- content that is generated on the service by means of an automated tool or algorithm in response to a prompt by a user and is only visible or audible to that user (no matter for how short a time).[15]

Generative AI

3.19 As set out in paragraph 3.9 above, pornographic content will also be treated as published or displayed on a service when it is generated on the service by means of an automated tool

[13] The BBFC defines tube services as free-to-access vide-sharing platforms "which allow users to upload and share videos with the public," in BBFC, 2023, Functionality of Online Pornography Services. A BBFC research report for Ofcom, p.10.
[14] Section 79(6)(b) of the Act. In relation to a search service, a 'search result' means "content presented to a user of the service by operation of the search engine in response to a search request made by the user" under section 57(3) of the Act. A 'combined service' is a "regulated user-to-user service that includes a public search engine" under section 4(7) of the Act.
[15] Section 79(6)(a) of the Act.

or algorithm within the service. This includes generative artificial intelligence (GenAI) tools which can create content in response to a prompt by a user. In this case, the Act makes clear that the person who makes available the automated tool or algorithm, by means of which content is generated, is to be regarded as having control over the content so generated. [16] That person is therefore treated as the provider of the service for the purposes of Part 5.

3.20 To illustrate further, if an online service provider makes available a GenAI tool that is designed to be used for the purpose of generating pornography, this aspect of the service would fall in scope of Part 5, and the duties outlined below will apply to it, provided the 'UK links' test under condition 3 is met.

3.21 If an online service provider makes available a GenAI tool that is not intended to be used for the purpose of generating pornography, the service provider should determine whether its tool is nonetheless capable of generating pornography. Where a tool is found to be capable of producing pornographic content, the service provider could implement one or more of safeguards suggested below to prevent their GenAI tool from generating pornographic content, to ensure it is not in scope of Part 5. The types of safeguards that could be explored may include, for example:

- the use of keyword blockers that prevent certain 'prompts' being entered into GenAI models (in this case, terms associated with pornography);
- content classifiers that can detect potentially pornographic content and prevent it from being shown to users;
- removing pornographic content from the datasets used to train GenAI tools;
- red teaming GenAI models to evaluate the strength of these and other safeguards, identifying where further improvements need to be made.[17]

3.22 We emphasise that, in order to ensure that the tool would not fall within scope of Part 5, the applicable safeguards would need to secure the outcome of preventing the creation of pornographic content. In that regard, we consider that solely including a provision in the terms of service for a GenAI tool that prohibits the tool being used to create pornographic content would not secure the outcome of preventing the type of content being produced, and would therefore not be deemed a sufficient safeguard.

3.23 The Part 5 duties may apply both to standalone GenAI services and to GenAI tools built into broader services with other functionalities. For example, it is possible that the Part 5 duties could apply to a chatbot that can generate audio-visual content which is built into a social media or pornography service.

3.24 However, where a service has functionalities that enables users who prompt the creation of content by GenAI tools to share that content with other users of the same service, this aspect of the service would be more likely to fall within scope of the Act's Part 3 duties.

[16] Section 226(15) of the Act.

[17] See Ofcom's discussion paper on red teaming for more detail on how this method can be used to evaluate the likelihood of a GenAI tool creating harmful or illegal content. Red Teaming for GenAI Harms, Ofcom (2024).

Condition 2: The service is not exempt

Which services are outside the scope of Part 5 or exempt?

3.25 There are certain types of services which fall outside the scope of Part 5. This is clear from section 80(2)(b) and (3) of the Act. As noted above, user-generated content on a U2U service (or combined service) and the search results on a search service (or combined service), are outside the scope of Part 5 and instead are regulated under the provisions of Part 3 of the Act.

3.26 Some providers of pornographic content may provide such content through an 'on-demand programme service.' This might include, for instance, a pornographic subscription service where editorial decisions about that service are made in the UK and the provider of the service has its head office in the UK. Part 5 does not apply in relation to a service to the extent it is an on-demand programme service within the meaning of section 368A of the Communications Act 2003 ("the 2003 Act").[18] Ofcom has provided guidance which sets out the statutory criteria for determining whether or not a service is an on-demand programme service. On-demand programme services are regulated under Part 4A of the 2003 Act, and Ofcom has set out Rules and Guidance for providers of on-demand programme services.

3.27 We have also set out guidance for on-demand programme service providers on measures to protect users from harmful material, which includes guidance on the specific rules relating to the protection of under-18s from harmful material.

3.28 There are also exemptions for services within the scope of Schedule 1 or Schedule 9 to the Act, the principal effect of which is to remove internal business services (e.g., intranet services) from Part 5, provided they meet the specified requirements in the Schedules.

Condition 3: The service "has links with the United Kingdom"

The two conditions for satisfying the UK links test

3.29 An internet service only falls within the scope of Part 5 of the Act if it "has links with the United Kingdom". For the purposes of Part 5 of the Act, the service only has such links if either of the following two conditions is met in relation to the service:

- the service has a significant number of United Kingdom users ("UK users");[19] or
- UK users form one of the target markets for the service, or the only target market.[20]

[18] Section 80(6) of the Act.
[19] Section 227(1) of the Act explains that, for the purposes of the Act, a user is a "United Kingdom user" of a service if either (a) where the user is an individual, the individual is in the United Kingdom; or (b) where the user is an entity, the entity is incorporated or formed under the law of any part of the United Kingdom.
[20] Section 80(4) of the Act.

What is a "significant number of UK users"?

3.30 The Act does not define what is meant by a 'significant number' of UK users for the purposes of considering the 'UK links' condition for the purposes of Part 5. Service providers should be able to explain their judgement, especially if they think they do not have a significant number of UK users.

3.31 We consider that the concept of "significant number of UK users" should be understood as meaning that the number of UK users on the service is material in the nature and context of the service in question, rather than the number of UK users of the service necessarily being a large or substantial number. We do not consider that the UK links test is intended to exclude services from the scope of the Part 5 duties simply because they have relatively small user bases, as this would not align with the purpose of the Part 5 duties which is to secure that children in the UK should not normally be able to encounter regulated provider pornographic content. We therefore suggest service providers err on the side of caution when assessing whether they have a significant number of UK users.

3.32 We also note that, under the Act, a user does not need to be registered to use the service in question to be counted as a user for the purposes of determining whether there is a significant number of UK users.[21] However, certain persons should not be counted for these purposes where they are acting in the course of the provider's business.[22] Whatever methodology a service provider uses to calculate user numbers, we expect providers to be able to distinguish between these types of users for the purposes of determining whether there is a significant number of UK users on the service.

When will the UK be a "target market" for a service?

3.33 While the Act does not define this expression, we consider that a 'target market' relates to a specific group of people (or organisations) that a provider is aiming its service toward. Our view is that there are a variety of factors which could indicate the UK is a target market for a service, including if the service in question:

- is designed for UK users;
- is promoted or marketed toward UK users;
- generates revenue from UK users either directly (e.g. via subscriptions or sales) or indirectly (e.g. through advertising to UK users, including people or organisations);
- includes functionalities or content that is tailored for UK users; or
- has a UK domain or provides a UK contact address and/or telephone contact number.

3.34 For the avoidance of doubt, a service could still meet the UK links test, if it has a significant number of UK users even if the UK is not a target market for that service. Alternatively, if the UK is a target market but the service does not have a significant number of UK users, the UK links test would be met in respect of that service.

[21] Section 227(2) of the Act.
[22] See section 227(3) and (4) of the Act.

4. The age assurance duties

Introduction to the age assurance duties

4.1 We have already explained in section 2 of this guidance that section 81 of the Act imposes the following core duties relating to age assurance on service providers in scope of Part 5:

- a duty to ensure, by the use of age verification or age estimation (or both), that children are not normally able to encounter content that is regulated provider pornographic content in relation to a service;[23] and
- the age verification or age estimation must be of such a kind, and used in such a way, that it is highly effective at correctly determining whether or not a particular user is a child.[24]

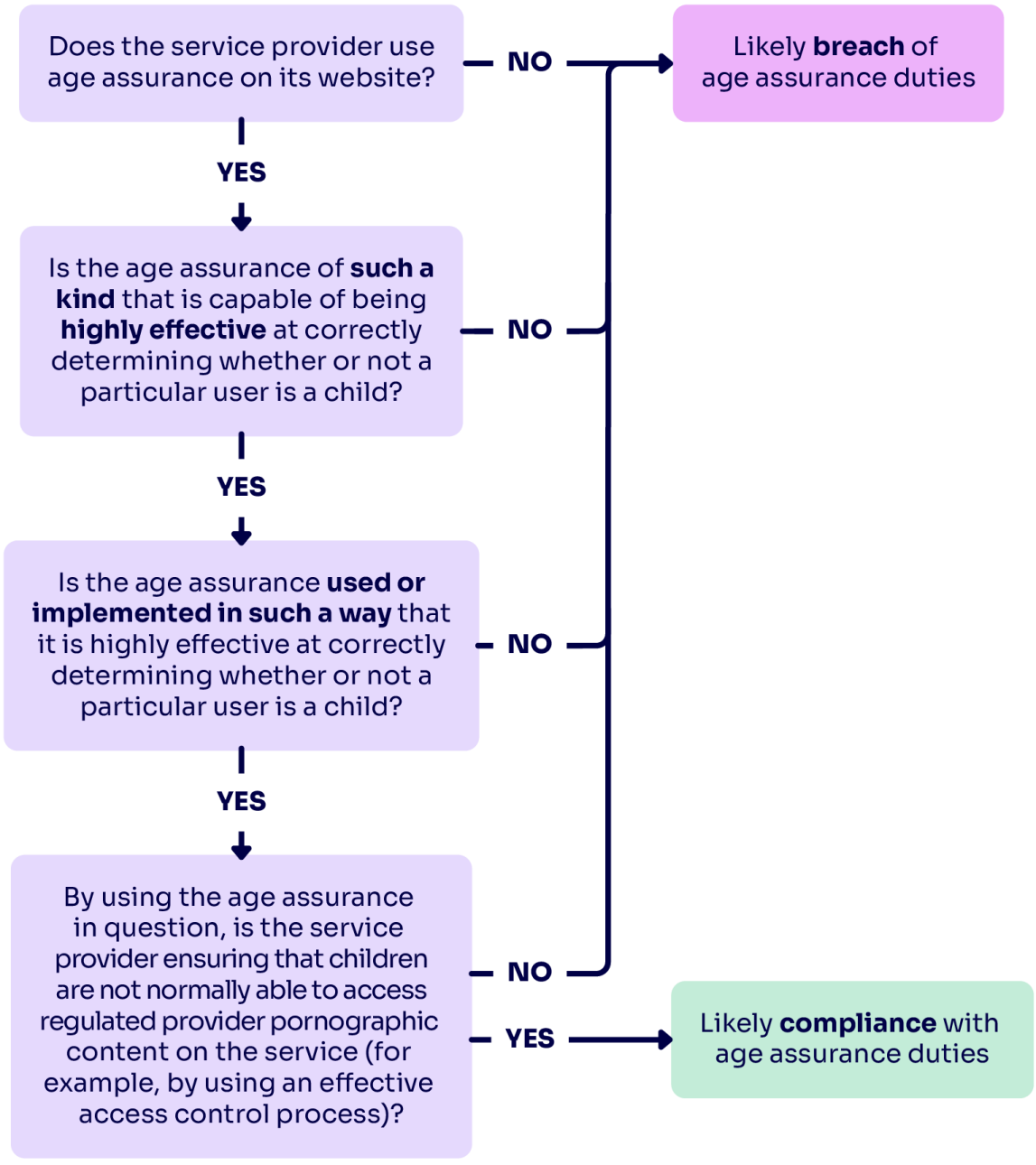
4.2 We refer in the rest of this guidance to those duties as the **'age assurance duties**'.

4.3 The general effect of the age assurance duties is to require service providers to deploy age assurance which is highly effective at determining whether or not a user is a child. Whenever a user has been determined not to be an adult, the provider must ensure that they are not able to encounter regulated provider pornographic content on the service. This means that the service provider must implement effective access controls to prevent users who have been determined by the age assurance process to be a child from encountering such content on the service (for example, by denying them access to any further sections of the service).

4.4 The following flow diagram shows – at a high level – the analytical framework Ofcom will use when assessing whether both of the age assurance duties have been met.

[23] Section 81(2) of the Act.
[24] Section 81(3) of the Act.

Figure 4.1: Analytical framework for assessing in-scope services' compliance with the age assurance duties.



4.5 In the rest of this section, we:

- outline the kinds of age assurance that we consider could be highly effective at correctly determining whether or not a user is a child, and those that are not capable of doing so;
- explain how service providers can use age assurance in such a way to ensure that it is, in practice, highly effective at correctly determining whether a user is a child by fulfilling certain criteria;

- set out certain principles that service providers should consider to ensure that the age assurance process is easy to use, and does not unduly prevent adult users from accessing legal content, where possible; and
- provide accompanying examples of non-compliance, to illustrate examples of circumstances in which we are likely to consider that a service provider has not complied with the age assurance duties.

Age assurance methods and processes

4.6 Throughout this guidance, we refer to age assurance **methods** and **processes.**

- An **age assurance method** refers to a particular system or technology that underpins an age assurance process.
- An **age assurance process** refers to the end-to-end process through which the age assurance method or combination of methods are implemented to determine whether or not a particular user is a child. The effectiveness of an age assurance method will depend on how it is implemented, including whether by itself or in combination with other methods. The age assurance process as a whole needs to be highly effective at correctly determining whether or not a particular user is a child.

Placement of age assurance check

4.7 To ensure that children are not normally able to encounter pornographic content, service providers must ensure that no pornographic content on their regulated service can be accessed by users before they verify their age. This means implementing age assurance at the point of entry to the site or ensuring that no regulated provider pornographic content is visible to users on entering the site before they have completed the age check.

Example of non-compliance with age assurance duties
Regulated provider pornographic content is visible to users on the regulated service prior to or during the process of completing an age check.

Kinds of age assurance

4.8 We set out below a non-exhaustive list of kinds of age assurance that we consider are capable of being highly effective at correctly determining whether or not a user is a child. [25] We recognise that age assurance methods are developing at pace and this list may expand in time. It is for the service provider to determine which age assurance method(s) to use in order to implement an age assurance process that is appropriate to meet its duties under the Act. Implementing one of the example methods is not a guarantee that the service is acting in accordance with the requirements of the Act – service providers need to be able to

[25] The kinds of age assurance in this list may be referred to by different names, and each kind may be implemented in a number of ways. We have used high-level descriptions to assist service providers in understanding the options that are available to them, but it is for each provider to consider which age assurance methods and processes will be most appropriate for complying with the duties.

demonstrate that the method has (or methods have) been implemented in such a way that ensures the overall process as a whole is highly effective.

4.9 We also provide examples of methods that we do not consider are capable of being highly effective at correctly determining whether or not a user is a child. Service providers should not rely on these methods alone to determine whether a user is a child in the absence of other measures. We would be likely to consider that the provider has not complied with either of the age assurance duties if it did so.

4.10 All age assurance methods involve the processing of personal data. As such, service providers who are required to implement age assurance are also subject to the requirements of the UK's data protection regime and should follow a data protection by design approach. The ICO has issued guidance on how these requirements should be met, as outlined in paragraphs 5.21 to 5.23, which will assist service providers to implement age assurance while protecting user privacy in line with the data protection regime.

4.11 Service providers have the flexibility to choose to build an in-house age assurance method or purchase a method from a third-party age assurance provider. Additionally, we recognise that there may be wider system-level age assurance methods that service providers could use to distinguish between children and adults on their service, for example, involving providers of devices, app stores, browsers operating systems, or relevant kinds of authentication systems. Regardless of where the age assurance occurs in the ecosystem or whether it is implemented by the service provider or by a third-party, it is the responsibility of the regulated service provider to ensure that age assurance is implemented in such a way that it is highly effective at determining whether or not a user is a child, in accordance with the age assurance duties. Should service providers opt to use wider system level age assurance, they must ensure the initial age check and the process to share this information with the regulated service (e.g. through age tokens) are highly effective.[26]

Kinds of age assurance that are capable of being highly effective

Open banking

4.12 This works by accessing the information a bank has on record regarding a user's age, with the user's consent. Confirmation of whether or not the user is over 18 is shared with the relying party.[27] The user's date of birth is not shared with the relying party, nor is any other information.

[26] Age tokens are reusable digital tokens that act as a digital proxy or representation of a completed age check. They can be shared by users across multiple services over a defined period of time as evidence that an age check has been completed.

[27] 'Relying party' refers to the service that is trying to establish the age of the user. In this context, the relying party is likely to be the regulated service.

Photo-identification (photo-ID) matching

4.13 This works by capturing relevant information from an uploaded photo-ID document and comparing it to an image of the user at the point of ID upload to verify that they are the same person.

Facial age estimation

4.14 This works by analysing the features of a user's face to estimate their age.

Mobile-network operator (MNO) age checks

4.15 Each of the UK's MNOs has agreed to a code of practice whereby they automatically apply a content restriction filter (CRF), which prevents children from accessing age-restricted websites over mobile internet on pay-as-you-go and contract SIMs. Users can remove the CRF by proving they are an adult.[28] MNO age checks rely on checking whether the CRF on a user's mobile phone has been removed. If the CRF has been removed, this indicates that the recorded user of the device is over 18. Confirmation of whether or not the recorded user is over 18, based on the status of the CRF, is shared with the relying party.

Credit card checks

4.16 In the UK, individuals must be 18 or over to obtain a credit card, therefore, credit card issuers are obliged to verify the age of applicants before providing them with a credit card.[29] Credit-card based age checks work by asking a user to input their credit card details, after which a payment processor sends a request to check the card is valid by the issuing bank. Approval by the issuing bank can be taken as evidence that the user is over 18.[30]

Email-based age estimation

4.17 These are solutions that estimate the age of a user by analysing the other online services where that user's provided email address has been used. This could include where an email address has been associated with financial institutions such as mortgage lenders.

Digital Identity Services

4.18 A digital identity is a digital representation of a person which enables them to prove who they are during interactions and transactions online and in person. Reusable digital identities are those which can be used multiple times for different interactions and transactions. This includes digital identity wallets which enable users to verify and securely store their attributes (such as age) in a digital format. This verification may take place using a variety of methods, including those listed above. Once their identity or an attribute of their identity has been verified and stored in the wallet, a user may choose to share individual attributes, such as their age, or their status as an adult, with a relying party.

[28] There are several ways to remove a CRF, depending on the MNO.
[29] We are aware that in the US, the term 'credit card' can be used to refer to debit cards. For clarity, when we refer to 'credit card' we mean cards tied to an account where money is borrowed and repaid, and not debit cards tied to current or 'checking' accounts, which often do not have the same 18+ requirements.
[30] Possession of credit card details is not evidence that the user is the credit card holder.

Kinds of age assurance that are not capable of being highly effective

Self-declaration of age

4.19 The Act states that measures which require users to self-declare their age (without other methods) are not to be regarded as age assurance.[31] These include:

- asking a user to input their date of birth without any further evidence to confirm this information; or
- asking a user to tick a box to confirm that they are 18 years of age or over.

Age verification through online payment methods which do not require a user to be over the age of 18

4.20 For example, debit cards or any other card where the card holder is not required to be 18.

General contractual restrictions on the use of the regulated service by children

4.21 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.

Example of non-compliance with age assurance duties

The service provider relies solely on self-declaration, general contractual restrictions or payment methods which do not require a user to be over 18, or a combination of these, to determine the age of users.

Criteria to ensure an age assurance process is highly effective

4.22 To ensure children are not normally able to encounter regulated provider pornographic content, service providers need to: (a) choose an appropriate kind (or kinds) of age assurance; and (b) implement it in such a way that it is highly effective at correctly determining whether a user is a child.

4.23 To ensure that an age assurance process is, in practice, highly effective at correctly determining whether or not a user is a child, service providers should ensure that the process fulfils **each** of the following four criteria:

- it is technically accurate;
- it is robust;

[31] Section 230(4) of the Act.

- it is reliable; and
- it is fair.

4.24 These criteria apply to the technical operation of the age assurance process. Table 4.2 below provides a summary of the criteria, all of which should be considered by service providers to decide their approach to age assurance. In addition to the summary in the table, we give more detail about each criterion below.

Table 4.2: Four criteria for ensuring an age assurance process is highly effective.

Criteria	Practical steps to fulfil criteria
Technical accuracy: the degree to which an age assurance method can correctly determine the age of a user under test lab conditions.	Ensure the age assurance method(s) has been evaluated against appropriate metrics and the results indicate that the method(s) is able to correctly determine whether or not a particular user is a child under test lab conditions. Include details of the performance of the method(s) against the metrics in the written record (see Section 5 below). Where the age assurance process used on the service involves the use of age estimation, the provider should use a challenge age approach. Periodically review whether the technical accuracy of the age assurance process for the service could be improved by making use of new technology and where appropriate, make changes to the age assurance process.
Robustness: the degree to which an age assurance method can correctly determine the age of a user in actual deployment contexts.	Implement age assurance processes that have undergone tests in multiple environments during development. Include details of this test process in the written record (see Section 5 below). Identify and take appropriate steps to mitigate against methods of circumvention that are easily accessible to children and where it is reasonable to assume that children may use them.

Criteria	Practical steps to fulfil criteria
Reliability: the degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.	Where age assurance methods forming part of the age assurance process rely on artificial intelligence or machine learning, take steps to ensure that: • the artificial intelligence or machine learning method(s) has been suitably tested during the development of the age assurance process to ensure it produces reproducible results; • once deployed, the artificial intelligence or machine learning method(s) is regularly monitored to ensure it produces reproducible results; • the outputs of the artificial intelligence or machine learning method(s) are assessed against key performance indicators designed to identify whether the artificial intelligence or machine learning produces reproducible results; • in circumstances where the artificial intelligence or machine learning used are observed to be producing unreliable or unexpected results, the root cause of the issue is identified and rectified. Take steps to ensure that any data relied upon as part of the age assurance process comes from a trustworthy source. Where using methods that rely on identity documents, record details of which identity documents they require or accept in the written record (see Section 5 below).
Fairness: the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.	Ensure that any elements of the age assurance process which rely on artificial intelligence or machine learning have been tested and trained on data sets which reflect the diversity in the target population. For methods reliant on artificial intelligence or machine learning, ensure the age assurance method(s) has been evaluated against the outcome / error parity and the results indicate that the method(s) do not produce significant bias or discriminatory outcomes.

4.25 We recognise that different kinds of age assurance – or even the same kinds of age assurance provided by different companies – may perform more strongly in some of these criteria than others. For example, one age assurance method could produce a highly reliable result due to limited variance, but it may provide greater opportunities for children to circumvent, therefore reducing its robustness. We expect to see that, when determining which age assurance method(s) to implement, service providers have satisfied themselves that the age assurance process as a whole fulfils each of the criteria.

4.26 Throughout this guidance we refer to the importance of testing. Testing plays a key role in how service providers can evidence that they have had regard to the four criteria. Where we suggest that service providers should consider testing, in all instances, metrics and results could be derived from testing by the service provider internally (if feasible), by their third-party age assurance provider(s), or by an independent third party. Where testing has been carried out by third parties, providers should understand what tests have been conducted and what metrics have been used to measure the results.

4.27 Service providers may choose to implement age assurance methods provided by services that are certified against a standard or scheme, such as the UK Digital Identity and Attributes Trust Framework ('the trust framework'). [32] The trust framework is a set of rules and standards governing the provision of digital verification services across the UK economy. Using a service certified against the trust framework (or any other standard or scheme) is not an automatic means of compliance, but it may help to evidence that a service provider has had regard to the four criteria to ensure that its approach is highly effective.

4.28 We give more details about each criterion below, including why the criteria are important, and steps service providers can take to have regard to them.

The technical accuracy criterion

What is technical accuracy?

4.29 Technical accuracy describes the degree to which an age assurance method can correctly determine the age or age range of a user under test lab conditions.

4.30 It is an indicator of the performance of an age assurance method and can be applied to methods that assess a user's age, age range, or whether a user is above a certain age.

Why is technical accuracy important?

4.31 An age assurance method which performs poorly in test conditions will perform worse in actual deployment contexts and is therefore very unlikely to be highly effective at correctly determining the age of users when deployed. This indicates that an alternative or additional age assurance method is likely to be required. Understanding the technical accuracy of the individual age assurance method(s) is therefore an important step in ensuring that the process as a whole is highly effective at correctly determining whether or not a particular user is a child.

[32] Office for Digital Identities and Attributes and Department for Science, Innovation and Technology, 'UK digital identity and attributes trust framework'. A register of certified services can be found on GOV.UK.

How can service providers have regard to technical accuracy?

Ensure the method(s) has been evaluated against appropriate metrics and the results indicate that the method(s) is able to correctly establish whether or not a particular user is a child

4.32 We expect service providers to evidence that they have taken steps to understand how technically accurate the age assurance method(s) they use is.

4.33 To understand the technical accuracy of an age assurance method, service providers should ensure it has been evaluated against appropriate metrics to assess the extent to which they can correctly determine the age or age range of a person under test lab conditions.

4.34 Age assurance methods either produce:

- a binary result (for example, categorising users as either over or under the age of 18); or
- a continuous result (for example, providing an estimation of the user's age).[33]

4.35 In the case of methods that produce a binary result, examples of appropriate metrics include but are not limited to; the True Positive Rate (TPR), False Positive Rate (FPR), and False Negative Rate (FNR).[34]

4.36 In the case of methods that produce a continuous result, examples of appropriate metrics include but are not limited to the Standard Deviation, Mean Absolute Percentage Error (MAPE), and Cumulative Score (CS).[35]

4.37 Service providers should be satisfied that the results indicate that the age assurance method(s) is able to correctly establish whether or not a particular user is a child and should record details of the assessment they made in relation to the above requirements. For further information on keeping a written record, providers should refer to Section 5.

Example of non-compliance with age assurance duties

The provider implements a process without evaluating any relevant performance metrics to understand the technical accuracy of the method(s) or is aware of evidence that relevant performance metrics suggest that the technical accuracy of a method(s) they are deploying is likely to be low. The result is that the chosen age assurance process routinely fails to correctly determine whether or not a particular user is a child, such that children are normally able to encounter pornographic content despite the presence of an age assurance process.

Use a challenge age approach for age estimation methods

4.38 Where the age assurance process used on the service involves the use of age estimation, the provider should use a challenge age approach.

4.39 A challenge age approach is widely used offline when selling age-restricted products in retail environments, for instance, through the retailing strategy 'Challenge 25.' In this approach, anyone who appears to the provider of restricted products to be under the age

[33] The estimation of the user's age will usually be accompanied by a confidence interval or range, which conveys the algorithm's level of uncertainty regarding the prediction. For example, where an age estimation method predicts that a user is 25 years old with a confidence interval of ±2 years, this means that the method estimates the user's age to fall within the range of 23 to 27 years.
[34] We define each of the metrics set out in the technical glossary in Annex 1 of this document.
[35] We define each of the metrics set out in the technical glossary in Annex 1 of this document.

of 25 should be challenged to provide acceptable ID proving that they are over the age of 18 if they wish to buy alcohol. The 'challenge age' in this scenario would be 25.[36]

4.40 In an online age assurance process, a challenge age approach refers to where a user who is estimated as being under a given challenge age must then undergo a second age assurance step (for example, a different age assurance method) to confirm that they are over the required age.[37]

4.41 The challenge age should be set at an appropriate level according to the limits of the technical accuracy of that method, for example, where system testing suggests that there is a significant risk of incorrectly estimating a 17-year-old's age by 7 years above or below. To manage this risk, a buffer can be set above the age by 8 years, so if the relevant age is 18 then the Challenge Age would be 25. For users estimated to be over the age of 25, no additional verification will be required. Where the method estimates that the user's age is under the challenge age, the user could be required to undergo another age check by a second method that is more technically accurate for that age group.

4.42 Using a challenge age approach helps to improve the overall effectiveness of the age assurance process by preventing or minimising borderline cases where the age estimation method incorrectly assesses a user as being an adult when they are a child.

Example of non-compliance with age assurance duties

The provider implements a process relying on age estimation without any challenge age mechanism or sets a challenge age inappropriately low, allowing a material number of children to successfully pass the test.

Periodically review the technical accuracy of the age assurance method(s) and make changes where necessary

4.43 We expect that the technical accuracy and testing practices of age assurance methods will continue to improve in years to come. Keeping a written record of the technical accuracy of their age assurance process will help service providers to understand how the effectiveness of their process compares against new technologies that may come onto the market. Providers should ensure their age assurance processes are reviewed and updated periodically to determine whether newer, more effective technologies and testing practices may provide a higher level of technical accuracy and, where appropriate, make changes to the age assurance process.

The robustness criterion

What is robustness?

4.44 Robustness describes the degree to which an age assurance method can correctly determine the age of a user in actual deployment contexts. Common threats to robustness in the context of age assurance methods include:

[36] Drink Aware, Challenge 25.
[37] ACCS, 2022. Measurement of Age Assurance Technologies.

- **conditions that change the quality or characteristics of the input** e.g., poor lighting, blurring, brightness, contrast, or positioning of the user in the image (relevant for methods reliant on visual input e.g., facial age estimation, photo-ID matching, etc).
- **circumvention techniques that are easily accessible to children where it is reasonable to assume they may use them** e.g., a child user uploading an image of an ID that does not belong to them.

4.45 We acknowledge that it may be possible for some children to circumvent the age assurance process or access control mechanisms that the provider has put in place to meet its duties. However, risks can be mitigated by service providers taking steps to improve the robustness of their age assurance process. We therefore expect service providers to take appropriate steps to mitigate against, and refrain from promoting, any methods of circumvention which are easily accessible to children and where it is reasonable to assume they may use them.

Why is robustness important?

4.46 Conditions in actual deployment contexts will vary considerably to those in a test scenario.

4.47 If the age assurance method is not robust, there are likely to be discrepancies in how it performs across varying conditions. For example, the performance of the method might be lower where a low-quality camera is used. Therefore, such a method would not be highly effective at correctly determining whether or not a user is a child as it does not perform consistently in a varied set of conditions.

4.48 In addition, there may be circumvention techniques which are easily accessible to children and where it is reasonable to assume that children may use them. If the age assurance process is not robust, it will be more vulnerable to circumvention. Therefore, the service provider will not be able to ensure that children are not normally able to encounter pornographic content.

How can service providers have regard to robustness when implementing age assurance?

Where relevant, ensure the technology has been tested in a range of conditions

4.49 We expect service providers to implement age assurance processes that have undergone testing to ensure the process is highly effective in a range of conditions; poor lighting, blurring, brightness, contrast, or positioning of the user in the image.

4.50 Should service providers choose an age assurance method dependent on visual or audio input, they should ensure that the technology underpinning that method has been tested in multiple environments during its development, to minimise any discrepancies in the performance of the method in actual deployment contexts.

4.51 Service providers could include details of this test process in their written record, as part of evidencing how they have chosen certain kinds of age assurance.

Identify and take appropriate steps to mitigate against methods of circumvention that are easily accessible to children and where it is reasonable to assume that children may use them

4.52 We expect service providers to identify and take appropriate steps to mitigate against methods of circumvention that are easily accessible to children, and where it is reasonable to assume that children may use them.

4.53 Where service providers implement age assurance processes that rely on details obtained via a user's identification documents, mobile phone number, email address, or credit card, we expect providers to have the means of checking that the details supplied belong to the user attempting to access the service.

4.54 Verifying the ownership of a user's details is one method of reducing the risk of a child user circumventing the age assurance process. For example, in the case of a mobile phone number, email address or credit card checks, this could be done through the use of a One Time Passcode (OTP) or multi-factor authentication.

4.55 Requiring a photo of the user at the point of ID upload when photo-ID matching helps to verify that the photo ID belongs to that user. Liveness detection provides further confidence that a child user has not uploaded a photo of an adult by ensuring that the user undergoing the age assurance process is present at the time the check is carried out.[38]

4.56 Liveness detection can also help to ensure that children are not using still images of adults to pass through facial age estimation.

4.57 It is possible to obtain fake forms of identification of varying degrees of sophistication. A robust photo-ID check should not be capable of being easily circumvented, and as such, a photo-ID method should be able to detect falsified documentation or manipulation that a child could create or obtain. Government-issued guidance on how to prove and verify someone's identity ("GPG45") provides some useful indicators on how a document can be scored to detect certain levels of faked documentation.[39]

4.58 Repeating an age check could also help to increase the robustness of an age assurance method, to prevent child access via device or account sharing and instances where children may be mistakenly classified as adults during the initial age check.

4.59 Service providers should determine whether repeated age checks are needed to secure the robustness of their solution based on the features of their service, and if so, how often it is appropriate to repeat an age check. For example, service providers may decide to age check each unique visitor to a service which does not require users to create an account. When deciding on the frequency of age checks, service providers should be mindful that data protection law requires them to assess the necessity and proportionality of the personal data processing and take a data protection by design approach to implementing the data protection principles.[40]

4.60 In addition, service providers should not publish content on their service that directs or encourages UK users to circumvent the age assurance process or the access controls, for example by providing information about or links to a virtual private network (VPN) which may be used by children to circumvent the relevant processes.

---

[38] Liveness detection is used to ensure that the face being analysed is not a photograph, video, or any other form of spoofed representation. The primary goal is to prevent attackers from using static images (print attack) or pre-recorded videos (replay attack) to trick the system into making inaccurate age estimates.

[39] Cabinet Office and Government Digital Service, 2023, Guidance – How to prove and verify someone's identity. Subsequent references to this document are referred to as 'GPG45.'

[40] ICO, 2023. Data protection by design and default.

Examples of non-compliance with age assurance duties

The service provider has not taken steps to mitigate against circumvention methods which are easily accessible by children, and where it is reasonable to assume they may use them. For example:

• the service provider has implemented facial age estimation which allows children to upload a still image they have obtained of an adult;

• the service provider has no way of ensuring that the details provided (e.g. via photo-ID, mobile phone number, email address, or credit card) belong to the user attempting to access the service;

• the service provider has implemented photo-ID matching which easily allows children to verify their age using fake or manipulated ID documents, or a still image they have obtained of an adult.

The service provider explicitly and deliberately encourages or enables child users to circumvent its age assurance process and/or access controls, e.g. by providing a link to and recommending the use of a VPN to avoid the controls, such that they are not likely to be effective at normally preventing children from encountering regulated provider pornographic content.

The reliability criterion

What is reliability?

4.61 Reliability describes the degree to which the age output from an age assurance method is reproducible and derived from trustworthy evidence.

4.62 Reproducibility describes the ability for an age assurance method to perform in a consistent manner, producing the same or similar outputs when given the same or similar inputs.[41]

4.63 Strength of evidence describes the relative weight that should be afforded to the underlying data or documents used as evidence for a user's age.[42] It concerns how trustworthy the documents or data are and therefore is indicative of how much reliance, or doubt, a service should place on the output of an age assurance method derived from this evidence.

Why is reliability important?

4.64 Without reliability, an age assurance method might correctly determine the same user to be a child in some instances, but not in others. Demonstrating that a method can account for variance and create reproducible outputs is therefore an important element of ensuring that children are not normally able to encounter pornographic content online.

[41] Gundersen OE, Kjensmo S, 2018, State of the art: Reproducibility in artificial intelligence in Proceedings of the AAAI Conference on Artificial Intelligence 32(1), p.1645.

[42] 'Strength' refers to evidence being harder to forge or counterfeit, as defined in GPG45.

4.65 In addition, where age assurance does not rely on trustworthy age evidence, there is a risk that children are granted access to the regulated service based on evidence that wrongly suggests they are over 18 in some instances.

How can service providers have regard to reliability when implementing age assurance?

Ensure that methods with a degree of variance have been suitably tested and that ongoing performance is measured and monitored

4.66 Age assurance methods that rely on artificial intelligence or machine learning, such as facial age estimation and photo-ID matching, are likely to produce outputs with a degree of variance. There are several reasons for this, including data variability and model complexity.

4.67 In addition, the performance of these specific methods may degrade over time due to 'model drift'. This is where the data the method has been trained on becomes less representative of the population using the age assurance method. For example, population demographics may shift over time resulting in a greater degree of variance.

4.68 Where service providers implement age assurance methods that rely on artificial intelligence or machine learning, we expect them to take steps to ensure that it that has been suitably tested during the development process to ensure it produces reproducible results, i.e. that outputs are consistently produced when the method is presented with the same inputs.

4.69 There should be regular monitoring and measurement of key performance indicators of the system once the age assurance process has been deployed.[43] Where necessary, root cause analysis and retraining should also be carried out where unexpected or unreliable predictions are being observed, particularly where such predictions may risk children being able to access pornographic content.

4.70 For other kinds of age assurance methods, including credit card age checks, open banking, and MNO age checks, outputs do not generally exhibit any variance of the type described above. In these cases, identical outputs should be produced when the method is presented with the same inputs. While reliability is less relevant for these methods, the service provider should still ensure that they fulfil the criteria of technical accuracy, robustness, and fairness.

Ensure that the evidence used is derived from a trustworthy source

4.71 We expect service providers to have confidence in the evidence that the age assurance method is relying on by considering, for example:

- the nature and properties of any identity documents, profiles, accounts, data, etc. used as part of the age assurance process; and

[43] For example:
1) Age Verification Accuracy Rate (AVAR): the percentage of users correctly identified as belonging to the appropriate age group;
2) Age Verification Efficiency (AVE): the time taken to complete the age verification process; and
3) Drift Threshold: establish predefined thresholds for AVAR and AVE beyond which significant model drifting is considered to have occurred.

- the source of the underlying data or documents.

4.72 In assessing the nature and properties of the relevant evidence, service providers should identify features that they would expect to see in a trustworthy source. When deploying photo-ID matching, for example, these features might include that:

- the evidence has originated from a country or organisation that is recognised as trustworthy;
- the positioning of the photographs on the evidence does not suggest they have been edited or replaced;
- the layout or any logos look as expected; and/or,
- the visible security features are genuine.[44]

4.73 Certification against the trust framework indicates that the evidence used by a third-party digital identity or attribute service provider should be reliable.[45]

4.74 Where service providers use methods that rely on identity documents, they should record details of which kinds of identity documents are required in their written record, as part of evidencing how they have used certain kinds of age assurance.

The Fairness criterion

What is fairness?

4.75 Fairness describes the extent to which an age assurance method avoids or minimises bias and discriminatory outcomes.[46] It refers here to the internal operation of an age assurance method, rather than external factors, such as a lack of access to a particular form of identification required by the age assurance method, which are covered by the principles below.

Why is fairness important?

4.76 Implementing a fair age assurance process is important to avoid discriminatory outcomes for certain groups. For example, an age assurance method that provides outputs with a lower degree of technical accuracy for users of certain ethnicities when relying on facial estimation.[47] Such an outcome might lead to children being incorrectly determined to be adult users, or adult users being incorrectly determined to be children.

[44] Further examples and information on checking that evidence is genuine or valid can be found in GPG45.
[45] Office for Digital Identities and Attributes and Department for Science, Innovation and Technology, 'UK digital identity and attributes trust framework'. A register of certified services can be found on GOV.UK.
[46] Fairness is a separate principle in data protection law, which states that that data should be processed lawfully, fairly and transparently. For more information, see ICO, Principle (a): Lawfulness, fairness and transparency and ICO, 2023. Guidance on AI and data protection.
[47] There may also be obligations for service providers under the Equality Act 2010 and guidance on this can be found at Equality and Human Rights Commission Guidance.

How can service providers have regard to fairness when implementing age assurance?

Ensure the technology has been tested on diverse datasets

4.77 We expect service providers to ensure that any elements of the age assurance process which rely on artificial intelligence or machine learning have been tested and trained on data sets which reflect the diversity in the target population.

Consider the outcome / error parity

4.78 Outcome / error parity can help service providers to understand how an age assurance method performs across groups with different characteristics, in order to mitigate bias and discriminatory outcomes.

4.79 A method's outcome parity can indicate that a model is fair if it produces equal numbers of positive or negative outcomes for different groups.

4.80 A method's error parity can indicate that a model is fair if it produces equal numbers of errors for different groups.

4.81 For methods reliant on artificial intelligence or machine learning, service providers should consider, monitor and make reference to outcome / error parity across different characteristics (such as race and sex) in their written record, as part of demonstrating how they have had regard to the fairness criterion.

4.82 Service providers should be satisfied that the results indicate that the age assurance method(s) does not produce significant bias or discriminatory outcomes.

Additional principles for providers to consider

4.83 Service providers should ultimately ensure that the age assurance process used is highly effective at correctly determining whether a particular user is a child.

4.84 Alongside fulfilling the criteria, the age assurance process should be easy to use and work for all users. Failing to do so might unduly prevent adult users from accessing legal content.

4.85 Service providers should therefore also consider the principles set out in Table 4.3 below when implementing age assurance methods or processes. We give more details about each principle below, including why they are important, and steps service providers can take to have regard to them.

Table 4.3: Summary table of the principles that services providers should consider in addition to the criteria.

Principles	Practical steps to consider principles
Accessibility: the principle that age assurance should be easy to use and work for all users, regardless of their characteristics or whether they are members of a certain group.	Assess the potential impact that the chosen age assurance method(s) might have on users sharing protected characteristics. Consider offering a variety of age assurance methods. Design the user journey through the age assurance process to be accessible for a wide range of abilities. Make information about the age assurance process available to the user prior to completing the age check.
Interoperability: the ability for technological systems to communicate with each other using common and standardised formats.	Stay up to date with developments in interoperable age assurance methods and use these approaches to reduce the burden on the user where possible and appropriate for the service.

Accessibility principle

What is accessibility?

4.86 The Act sets out that Ofcom's guidance to assist service providers in complying with the Part 5 duties may elaborate on:

- the principle that age verification or age estimation should be easy to use;
- the principle that age assurance should work effectively for all users regardless of their characteristics or whether they are members of a certain group.[48]

4.87 We refer to these principles collectively using the term **accessibility.**

Why is accessibility important?

4.88 Age assurance processes that are inaccessible either because they are complex, are less accurate for users with different characteristics, or include requirements that certain groups of users are unable to fulfil or understand, may result in users being unable to access a service that they should otherwise be able to use.

[48] Section 82(3)(a) and (b) of the Act.

4.89 To enhance accessibility, it is also important to explain to users what the age assurance process is designed to do and how it works, so that users can understand why it is necessary and how to complete the process.

How can service providers have regard to accessibility when implementing age assurance?

4.90 It is for service providers to consider what steps are most appropriate for their service to take to ensure their age assurance process is accessible. Examples of practical steps to improve accessibility could include:

- assessing the impact that the age assurance process might have on users sharing protected characteristics and including details of this assessment in the written record;
- offering more than one age assurance method to assist users who may be unable to, or may find it more difficult to, use certain kinds of age assurance;[49]
- designing the user journey through the age assurance process to be accessible for a wide range of abilities. This might include, for instance, ensuring that users with visual impairments are able to use screen readers to complete the age assurance process, or ensuring that all functionality is available from a keyboard for users with limited motor control; or
- making information about the age assurance process available in the form of a pop up prior to completing the age check, for example, as a smaller, new window that appears overlayed on top of the webpage, drawing the user's attention. The text could be included in this window, or the pop up could feature a button prompting users to click for more information.[50]

4.91 The Web Accessibility Initiative's Web Content Accessibility Guidelines provide recommendations for how service providers can make services more accessible to disabled people.[51]

Interoperability principle

What is interoperability?

4.92 The Act sets out that Ofcom's guidance to assist service providers in complying with the Part 5 duties may elaborate on the principle of interoperability between different kinds of age assurance.[52]

4.93 Interoperability describes the ability for technological systems to communicate with each other using common and standardised formats. It relies on consistent technological

[49] For example, those without credit cards will be unable to complete a credit card check. Those without a driving licence or passport will be unable to undergo a photo-ID check that relies on these documents.
[50] This could be part of a service provider's publicly available statement, which we provide more guidance on in Section 6 (5.28-5.5.30).
[51] Further guidance on businesses' legal obligations in this area can be found at Equality and Human Rights Commission Guidance.
[52] Section 82(3)(c) of the Act.

approaches being adopted across different methods. Standards, technical frameworks and other specifications are important to achieving interoperability.

4.94 In the context of age assurance, interoperability may involve re-using the result of an age check across multiple services allowing different providers of age assurance methods to share the information, provided this is done in line with data protection laws.

Why is interoperability important?

4.95 The principle of interoperability offers a potential benefit to the user experience, as it limits the amount of information that users need to provide when accessing a new service if they have already proved their age elsewhere. This could reduce the time and effort required by users to understand, and input into, different age assurance processes.

How can regulated services have regard to interoperability?

Stay up to date with developments in interoperability

4.96 We recognise that the development of interoperable solutions is still at an early stage. Service providers can have regard to interoperability by staying up to date with developments in this area, and considering whether to implement interoperable solutions to age assurance where they exist and are appropriate for the service.

4.97 Current efforts at enabling interoperable age assurance include the euCONSENT project, a non-profit non-governmental organisation that has been established with the intention of designing, testing, and implementing extensions to the eIDAS infrastructure to enable open-system, secure and certified interoperable age assurance.

Illustrative case study

4.98 In Table 4.3 below, we provide an illustrative case study to explain how the criteria and principles set out in this section of the guidance might apply to an age assurance process.

4.99 Many alternative approaches to age assurance exist, and different approaches may be more suitable for different services. The case study contains an example that is intended only to illustrate how the criteria apply to assist service providers in complying with their duties relating to age assurance. This example should not be read as endorsing one particular age assurance method or process, nor should it be read as determinative that the given approach would be highly effective. Providers should decide what is the most appropriate method/process for their regulated service to ensure that children are not normally able to encounter pornographic content. Adhering to the process highlighted below is in no way determinative of compliance with the Part 5 duties – service providers need to be able to demonstrate that, as a result, children are not normally able to access pornographic content in their services.

Table 4.4: An illustrative case study of how the criteria and principles might be applied to the age assurance process.

High-Level User Journey	Service provider considerations
(1) On accessing the regulated pornography service, a pop-up	The service provider has ensured pornographic content is not visible prior to verifying the age of the user, to ensure

High-Level User Journey	Service provider considerations
asks the user to confirm their age.	children are not normally able to encounter pornographic content. It designs a pop-up box for the age assurance process that appears as a new, smaller window overlayed on top of the webpage that the user is viewing.
(2) The pop-up contains: **(a) Information on all the kinds of age assurance used, and how the processes work, in accessible language;** **(b) A link to more detailed information, including relevant transparency information as per the requirements in the UK General Data Protection Regulation (UK GDPR);** **(c) A box reading "Understood – continue to age assurance."**	The service provider has set out a publicly available statement for its users explaining its age assurance process, as required by section 81(5) of the Act. Including this statement, or access to this statement, in the age assurance pop-up ensures that users can read the summary prior to the age assurance check, as outlined in paragraph 5.28 of this guidance.
(3) The user is directed to an age estimation check. At the bottom of the screen, the user can click on a link reading "prove my age another way." **During the age estimation process, the user is prompted to take steps to ensure the age estimation works effectively (e.g., ensure the lighting is appropriate).** **If the age estimation method estimates that the user's age is over a certain challenge age, they are granted access to the site without further requirements.**	The service provider chooses an age estimation method and carries out the following checks against Ofcom's criteria. The estimation method could be purchased from a third-party age assurance provider or developed internally but the platform must ensure in either case the relevant checks are carried out to assess if the method is highly effective. • Technical accuracy – The service provider assesses the results of performance testing of the age estimation method and determines that the level of technical accuracy is not high enough for users with an age close to 18, and a challenge age is needed. The service provider adds a secondary method to the age assurance process as described in the next section of this table. • Robustness – The service provider carries out testing in a range of conditions to ensure that the estimation method performs to a suitable level in practice. It also determines that the method is not susceptible to any circumvention techniques that are easily accessible to children – for example, it uses presence detection. • Reliability – The service provider repeats the testing undertaken in the steps above. It selects a timeframe to conduct this testing that is derived

High-Level User Journey	Service provider considerations
	from their assessment of the risks. Additionally, it closely monitors the ongoing performance and outputs of the method by, for example, noting any trends of inaccurate age estimations and/or a rise in complaints/appeals. Undertaking additional subsequent testing, monitoring performance and taking necessary remedial action promptly, should ensure that the service provider maintains the initial performance it observed. • Fairness – The service provider ensured that during development of the solution, steps were taken to train the model on a diverse dataset. When considering test results, it ensures that performance across different protected characteristics has minimal variations.
(4) If the age estimation method determines that the user's age is lower than the challenge age, then the user must undergo an age verification check.	The service provider, having assessed that the estimation method is not sufficiently technically accurate for users whose age is close to 18, decides to choose an age verification method for those users. The verification method could be purchased from a third-party age assurance provider or developed internally, but the platform should ensure the relevant checks are carried out and recorded to assess if the method is highly effective. • Technical accuracy – The service provider assesses the results of performance testing of potential age verification methods and chooses one (or more) that provide(s) a high level of technical accuracy. • Robustness – The service provider chooses a verification method that sufficiently guards against fake input and sufficiently binds the proof of age to the user presenting for the age check. • Reliability – The service provider takes steps to ensure that the chosen secondary age assurance method performs consistently. For example, this may mean ensuring that the method can identify new or updated identification documents, or identification documents from non-UK territories. It also means, as with the solution above, that periodic testing is undertaken to ensure consistent performance. • Fairness – The service provider undertakes an assessment to ensure that the method performs to an equivalent level of accuracy for users with different characteristics.

High-Level User Journey	Service provider considerations
	Once the service provider has determined that its age assurance process as a whole is highly effective, it then considers the guidance principles to ensure the process is easy to use and does not unduly exclude adult users: • Accessibility – The service provider considers the impact of the age assurance process on users with different characteristics. While it considers that having a secondary method mitigates the potential negative impact for young adults who look younger than 18 if relying on facial age estimation, it identifies that the overall user journey may be difficult to use for users with disabilities. It consults the Web Content Accessibility Guidelines and implements relevant measures to make the age assurance process easier to use, such as reducing the complexity of the text guiding users through the age checks by shortening sentences and using bulleted lists where appropriate. • In addition, the provider carries out an assessment to understand the proportion of users who would likely possess the necessary proof to verify their age and whether implementing this method would cause a disproportionate number of specific users to be excluded. The service provider decides that that a large volume of users could verify their age in this way with minimal negative impact. • Interoperability – The service provider looks into the current efforts to enable interoperable age assurance. It identifies a project that may be appropriate for its service and may help to reduce the potential burden on users. The provider decides to regularly review the project status to determine if is ready to implement. To comply with their requirements under the UK GDPR, the service provider should provide a means for people to challenge age estimation or age verification results which they know to be inaccurate.[53]
(5) If the age estimation method determines that the user's age is equal to or higher than the challenge age, or if the age	The service provider continues to monitor the performance of both methods and, by doing this, its overall age assurance process using suitable testing and analysis, and ensures that it takes action to remedy identified problems

[53] See ICO, Section 3 of the Commissioner's Opinion on Age Assurance.

High-Level User Journey	Service provider considerations
verification method determines that the user's age is 18 or above, the user's access to pornographic content is enabled. Otherwise, the provider denies the user who has failed the relevant age check access to any part of the service that hosts regulated provider pornographic content.	which could result in the age assurance process not being highly effective.

5. Duties to keep written records for age assurance

Age assurance record-keeping duties

5.1 The Act sets out the following duties relating to record keeping:

- A duty to make and keep a written record, in an easily understandable form, of –
  - the kinds of age verification or age estimation used, and how they are used; [54] and
  - the way in which the service provider, when deciding on the kinds of age verification or age estimation and how they should be used, has had regard to the importance of protecting UK users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a regulated service (including, but not limited to, any such provision or rule concerning the processing of personal data),[55]
- A duty to summarise the written record in a publicly available statement, so far as the record concerns compliance with the duty set out in section 81(2), including details about which kinds of age verification or age estimation a service provider is using and how they are used.[56]

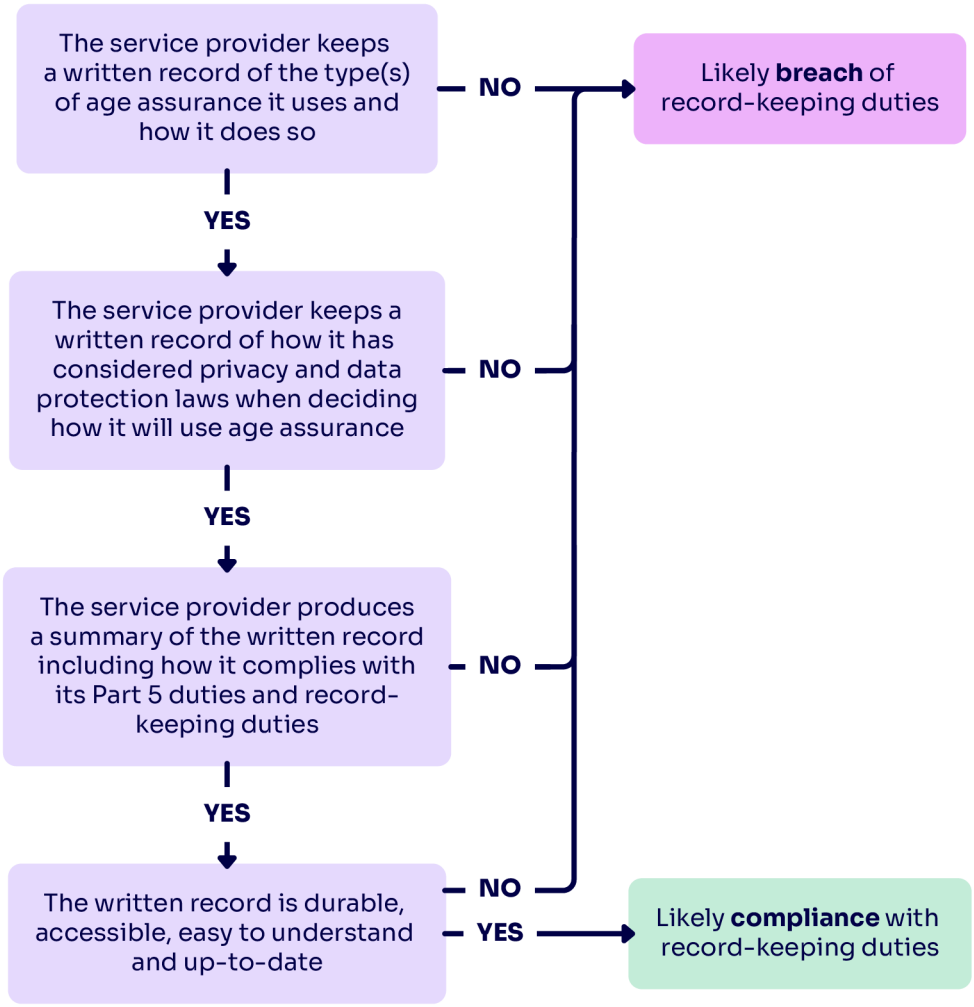
5.2 We refer in the rest of this guidance to those duties as the **'record-keeping duties.'** These requirements can be broken down into the following core elements:

- the service provider keeps a written record of the type or types of age assurance it uses and how it does so;
- the service provider keeps a written record of how it has considered privacy and data protection laws when making a decision as to how it will use age assurance;
- the service provider produces a summary of the parts of the written record that relate to how it has complied with the duty set out in section 81(2) of the Act;
- the summary in question includes details of the types of age assurance the service provider uses and how it does so; and
- the summary is available to the general public.

5.3 Figure 5.1 below contains a diagram with an overview of the analytical framework that Ofcom will use in assessing service providers' compliance with their record-keeping duties.

[54] Section 81(4)(a) of the Act.
[55] Section 81(4)(b) of the Act.
[56] Section 81(5) of the Act.

Figure 5.1: Analytical framework for assessing in scope services' compliance with the record-keeping duties.



5.4 We provide guidance below to assist service providers in complying with each of these elements. As well as guidance on how to keep a written record effectively, it covers what to include in a written record of the kinds of age assurance used and how they are used, and in a written record of having regard to user privacy. In addition, we provide guidance on making a publicly available statement. We also set out examples of circumstances where we are likely to consider that a service provider has not complied with its record keeping duties.

How to keep a written record on age assurance

5.5 The written record which a service provider keeps of the age assurance process it uses must be durable, accessible, easy to understand and up-to-date.

5.6 Written records can be made and kept in a durable medium of the service provider's choice (for example, on a computer or using any storage device such as a CD-ROM, USB memory

stick, cloud storage, a network drive, or a paper copy), which is capable of being provided easily and quickly to Ofcom if required.

5.7 Written records should be legible and written in as simple and clear language as possible. They should not include jargon, encryption, shorthand or code such that Ofcom cannot understand what they say.

5.8 Where reasonably practicable, written records should be kept in English (or for service providers based in Wales, in English or Welsh). If this is not reasonably practicable, the records must be capable of being translated into English.

Example of non-compliance with age assurance duties

The written record is written in an incomprehensible format that means it cannot be easily understood by Ofcom.

5.9 The service provider must keep a written record of the current age assurance process that it deploys to comply with the age assurance duties. Providers should make the record as soon as possible after the deployment of any new method and keep it updated to ensure it remains current.

Example of non-compliance with age assurance duties

The service provider has not updated its written record to ensure it remains current.

5.10 It is important that earlier versions of the record are retained so that the provider can provide both current and historic records of how it has complied with the age assurance duty.

5.11 Written records should be dated when they are made and on each occasion that they are updated.

5.12 For the avoidance of doubt, providers are not required by the Act to keep a record of the result of any individual age check, such as a user's age or date of birth. No personal data about users should be included in the written record.

5.13 Service providers should retain written records in accordance with their record retention policies, or a minimum of three years (either calendar or financial), whichever is the longer, even though there may have been subsequent revisions to reflect changes to the service provider's compliance measures. This will ensure that the provider is able to provide both current and historic records of how it has complied with the relevant duties.

On the kinds of age assurance used and how they are used

5.14 When making and keeping a record of the kinds of age assurance used, and how they have used them, service providers should detail:

- any third-party supplier contracted to provide an age assurance process;
- what kind of age assurance the process uses (whether consisting of one or multiple methods).

5.15 We expect service providers to include in their written record how each method or combination of methods fulfils the criteria and principles set out in Section 4. In Section 4,

we have set out ways in which providers can have regard to the criteria and principles when implementing age assurance.

Example of non-compliance

The service provider has not described, in its written record, the kinds of age assurance method(s) it uses, or how they are used, to ensure that children are not normally able to encounter regulated provider pornographic content on its regulated service(s).

On having regard to privacy and data protection

5.16 For an understanding of how to have regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy, service providers should familiarise themselves with the data protection legislation, and how to apply it to their age assurance method. This includes by consulting ICO guidance and seeking relevant independent legal advice as service providers deem appropriate.

The Data Protection Regime

5.17 The UK data protection regime is made up of several pieces of legislation, including the Data Protection Act ("DPA") 2018, the UK GDPR, and the Privacy and Electronic Communications Regulations ("PECR") 2003. Taking data protection requirements into account will help service providers to meet the record-keeping duty related to privacy set out at paragraph 5.1(ii).

5.18 Together, this legislation provides a risk-based framework for making sure the processing of personal data respects the fundamental rights and freedom of individuals. The ICO is responsible for upholding information rights through its oversight and enforcement of the legislation.

5.19 Service providers should consult ICO guidance to understand how to comply with the data protection regime, including its guides to the data protection principles, identifying an appropriate lawful basis, and how to respond to users exercising their individual rights afforded by the UK GDPR.[57]

5.20 The PECR will apply to anyone who stores information on or gains access to information on a user's device, for example, by using cookies or other similar technologies. Where an organisation stores, or gains access to, information on a user's device, for example, by using cookies or other similar technologies, PECR will apply. The ICO has produced detailed guidance on this topic.

ICO guidance on data protection and age assurance

5.21 The data protection principles are the cornerstone of the UK GDPR.[58] They apply whenever services process personal data, including for the purposes of age assurance. The principles are:

[57] ICO, 2023. A guide to the data protection principles; ICO, A guide to lawful basis; and ICO, Individual rights – guidance and resources. ICO Guidance on controllers/ processors.

[58] For an overview of each principle, see the ICO's guide to the data protection principles.

- Lawfulness, fairness and transparency;[59]
- Purpose limitation;[60]
- Data minimisation;[61]
- Accuracy;[62]
- Storage limitation;[63]
- Security;[64] and
- Accountability.[65]

5.22 Before compiling a written record for the purposes of compliance with the duties set out in the Act, service providers should familiarise themselves with the Commissioner's Opinion on Age Assurance for the Children's code ("the Opinion"), which outlines how the data protection principles and other requirements can be considered in the context of age assurance. The considerations set out in the Opinion are technology neutral, making them applicable to any kind of age assurance.[66]

5.23 Consulting the Opinion will help service providers implement age assurance while protecting user privacy in line with the data protection regime. This will help service providers to keep a written record of how they have regard to the importance of protecting UK users from a breach of any statutory provision or rule of law concerning privacy.

Examples of how to keep a written record regarding protecting user privacy

5.24 When considering compliance, Ofcom will consider whether service providers have kept a written record of how they have had regard to privacy and data protection requirements in making decisions around age assurance. Where we have concerns that a provider, based on its written record, has not complied with its obligations under data protection laws, we may refer the matter to the ICO.

5.25 The examples listed below are ways to demonstrate compliance with data protection law, which can also help service providers to comply with the written record duty in relation to privacy under the Act.

- **Conducting a Data Protection Impact Assessment (DPIA).** These are required by data protection law where processing is likely to result in a high risk to the rights and freedoms of individuals. DPIAs will assist service providers in identifying and mitigating the risks arising from their processing of personal data, which can help demonstrate that they have had regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy. ICO guidance states that providers should identify and assess risks, and identify options for reducing said risks. Detailed

[59] ICO, Principle (a): Lawfulness, fairness and transparency.
[60] ICO, Principle (b): Purpose limitation.
[61] ICO, Principle (c): Data minimisation.
[62] ICO, Principle (d): Accuracy.
[63] ICO, Principle (e): Storage limitation.
[64] ICO, Principle (f): Integrity and confidentiality (security).
[65] ICO, Accountability and governance.
[66] See ICO, Section 6 of the Commissioner's Opinion on Age Assurance.

guidance on how to carry out a DPIA, and a sample template, can be found on the ICO website.

- **Providing privacy information to users.** Service providers should give users information about why they need to provide any personal data, how it will be processed, how long it will be retained, and if it will be shared with anyone else. More information on privacy notices can be found on the ICO website.[67]
- **Keeping written records of processing activities.** Most organisations that process personal data must document their processing activities.[68]
- **Having up to date data protection policies along with a record of how providers make staff aware of them.** This provides staff with clarity and consistency around their data protection obligations.[69]
- **Having a record of which staff have completed any data protection training programme that is in place.** This helps to ensure all staff have adequate knowledge of data protection, as appropriate for their role.[70]
- **Clearly documenting technical and organisational security measures**.[71]

Example of non-compliance with age assurance duties

There is no mention of how the service provider has had regard to the importance of protecting the privacy of UK users in its written record.

Making a publicly available statement

5.26 The Act requires service providers to set out in a publicly available statement a summary of the kind(s) of age assurance used and how they have used it, as described in their written record.[72] The Act defines 'publicly available' as "available to members of the public in the UK."[73]

5.27 In summarising the written record, the service provider should aim to provide the main details about the age assurance process which it uses. This will help to explain to users of the regulated service what the process is designed to do and how it works, so that users can understand why it is necessary and how to complete the process. This will also support the accessibility principle. In addition, the provider should omit any information which is commercially sensitive. We also recommend providers to identify and omit from the summary any information which might pose a security risk to the service or other relevant parties, or any information which might expose the age assurance process to increased risk of circumvention, if made available to the public.

[67] See ICO, Transparency (cookies and privacy notices), and ICO, How to write a privacy notice and what goes in it.
[68] ICO, Records of processing and lawful basis.
[69] ICO, Policies and procedures.
[70] ICO, Training and awareness.
[71] ICO, A guide to data security.
[72] Section 81(5) of the Act.
[73] See section 236 of the Act.

5.28 Service providers should ensure that the statement is available to members of the UK general public in an easy to find area of the regulated service that is clearly labelled and accessible to users from the point that they first access the service. For instance, the section at the top (header) or bottom (footer) of the webpage, where users can typically find site contact details and navigation links. The header and footer are generally displayed on every page of the website, so are easily accessible. To ensure that users can read the summary prior to completing the age assurance check, providers should include the summary alongside any explanatory text on how the age assurance process works. This could be in the form of a pop-up; for example, a smaller, new window that appears overlayed on top of the webpage, drawing the user's attention. The summary text could be included in this window, or the pop-up could feature a button prompting users to click for more information.

5.29 Service providers should write the statement in accessible language that is formatted in a way that helps the public to understand the kinds of age assurance used and how they have been used.

5.30 Service providers should design the statement for the purposes of ensuring usability for users with disabilities who rely on assistive technologies to use the internet. [74] For example:

- ensuring that all functionality for accessing the statement is available from a keyboard, to allow users with limited fine motor control to use keyboard navigation technology instead; or
- providing alternative text for any images used within the statement to allow users with visual impairments to use a screen reader, which reads aloud the information on the page.[75]

Example of non-compliance with age assurance duties

The service provider has not summarised its written record in a publicly available statement, or the statement is not available to users.

[74] The Assistive Technology Industry Association (ATIA) defines assistive technology as "any item, piece of equipment, software program, or product system that is used to increase, maintain, or improve the functional capabilities of persons with disabilities" ATIA, What is AT?

[75] Web Accessibility Initiative, 2022, Introduction to Web Accessibility.

6. Assessing compliance with age assurance and record-keeping duties

Introduction

6.1 In this section, we set out an overview of our general approach to enforcement under the Act, including the principles that we will consider when determining whether a service provider has complied with the duties.

6.2 We also set out where service providers can find further information about our enforcement processes relating to the Act.

Possible enforcement action and sanctions

6.3 The Act gives Ofcom the power to take enforcement action, including imposing financial penalties of up to £18 million, or 10% of qualifying worldwide revenues (whichever is greater), where we find that service providers have failed to comply with their Part 5 duties.[76] Sections 4 and 5 of this guidance provide the analytical frameworks Ofcom will typically apply when assessing whether the Part 5 duties have been met and examples of where we are likely to consider that a regulated service has not complied.

6.4 When assessing compliance, we will act in accordance with our general duties, including our duty to have regard to our regulatory principles of transparency, accountability, proportionality, consistency and ensuring that regulatory action is targeted only at cases which require it.[77]

Ofcom's specific Online Safety Enforcement Guidance

6.5 Our Online Safety Enforcement Guidance ("OS Enforcement Guidance") sets out the procedures we will follow where we suspect non-compliance with the obligations that apply to service providers under the Act. It also outlines the different enforcement tools that we may use and explains how we prioritise cases that come to our attention, according to:

- the risk of harm or seriousness of the alleged conduct and any impact this may have on the risk of harm presented by content available on the regulated service;[78]
- the strategic significance of addressing the conduct; and

[76] Paragraph 4 of Schedule 13 to the Act.
[77] Section 3(3)(a) of the CA03.
[78] In this context, seriousness includes whether the conduct is, or appears to be "a repeated, intentional, systemic, or particularly flagrant contravention."

- the resource implications and risks in taking enforcement action.

6.6 Section 3(4A) of the Communications Act 2003 ("CA03") requires us to have regard to, among other matters, the need for a higher level of protection for children than for adults.[79] Section 151(3) of the Act also states that our enforcement guidance must include an explanation of how we will take account of the impact (or possible impact) of non-compliance on children.

6.7 We will include the harm or risk of harm to children in our prioritisation framework when considering:

- the risk of harm or seriousness of the conduct; and
- the strategic significance of addressing the alleged contravention.

6.8 The inclusion of the risk of harm to children in two parts of Ofcom's prioritisation framework reflects the importance of this factor in considering whether or not to take enforcement action.

[79] As amended by the Act. Section 3(4)(h) of the CA03 also requires us to have regard to the vulnerability of children in performing our duties.

A1. Glossary

Technical glossary

Metrics used to measure the accuracy of age assurance

Term	Meaning
Absolute error (AE)	The same as the 'error,' but disregards the sign (i.e., positive or negative) thus focusing only on the magnitude (size) of the difference between the technologically-determined age and actual age.
Accuracy (ACC)	The fraction of the predictions the model got right. The formula is ACC = (TP + TN) / (TP+ TN + FP + FN).
Cumulative score (CS)	An aggregated score that is calculated by summing the individual score across over a period of time/category etc.
Error	The user's age determined by the technology minus the user's actual age. An overestimation yields a positive value, whereas an underestimation yields a negative value.
False negative (FN)	An outcome where a model incorrectly predicts a negative class i.e., a user is under 18 and the model predicts their age 18 or over.
False negative rate (FNR) / Miss rate	Measures the proportion of FN against all negative predictions (i.e., FN and TP). FPR highlights the performance of the model in yielding FP results and this should be minimised. The formula is FNR = FN / (FN + TP).
False positives (FP)	For the purpose of age assurance, this refers to an outcome where a model incorrectly predicts a positive class i.e., a user is 18 or over and the model predicts their age as under 18.
False positive rate (FPR)	Measures the proportion of FP against all positive predictions (i.e., FP and TN). FPR highlights the performance of the model in yielding FP results and this should be minimised. The formula is FPR = FP / (FP + TN).
Mean absolute error (MAE)	The central value of the absolute error. It describes the average discrepancy between a user's technology determined age and their actual age, ignoring whether it is an over- or under-estimation. It is calculated by summing the absolute errors for a given number of absolute errors, then dividing this by the number of absolute errors. The formula is MAE = $(1/n)\ \Sigma(i=1 \text{ to } n)\ \lvert y - x \rvert$ where n = number of observations in the dataset, y = is the true value, x = is the predicted value.

Term	Meaning
Mean absolute percentage error (MAPE)	A metric that used to measure the accuracy in a regression analysis, this is useful where relative errors (age range estimations) are more meaningful than absolute errors. M = (1/n) Σ(t=1 to n)|(At – Ft) / At) |* 100 Where n = number of times the summation iteration happens, At = actual value and Ft = forecast value.
Outcome / error parity	Outcome / error parity is a measure designed to compare how an age assurance process outcome impacts users in different groups, both positively and negatively, and/or how often these different groups of users are subjected to errors.
Standard deviation (SD)	A measure of variation or dispersion of the dataset relative to the mean. A low SD suggests datapoints closer to the mean, whereas a high SD suggests datapoints are more dispersed. s = ∑((X − MAE)^2/(n – 1)) where X = is the i*th* point in the dataset, MAE = is the mean absolute error, and n = the number of datapoints in the dataset.
True positives (TP)	An outcome where a model correctly predicts a positive class i.e., a user is under 18 and model predicts their age as under 18.
True positive rate (TPR) / Recall	For the purpose of age assurance, this measures the proportion of TP predictions out of all actual positive instances (i.e., TP and FN). This metric highlights the model's performance in correctly identifying positive cases. The formula is TPR = TP / (TP + FN).

Terms used in this guidance

Statutory definitions

Term	Meaning
'Age estimation'	"Any measure designed to estimate the age or age-range of users of a regulated service."[80]
'Age verification'	"Any measure designed to verify the exact age of users of a regulated service."[81]
'Child'	"A person under the age of 18."[82]

[80] Section 230(3) of the Act.
[81] Section 230(2) of the Act.
[82] Section 236(1) of the Act.

Term	Meaning
'Provider'	"The entity that has control over which content is published or displayed on the service." Where an individual or individuals have control over which content is published or displayed, rather than an entity, "the provider of the service is to be treated as being that individual or those individuals."[83] "The provider of an internet service that is generated by a machine is to be treated as being the entity that controls the machine (and that entity alone.)" "If no entity controls the machine, but an individual or individuals control it, the provider of the internet service is to be treated as being that individual or those individuals."[84]
'Provider pornographic content'	In relation to an internet service, "pornographic content that is published or displayed on a service by the provider of the service or by a person acting on behalf of the provider, including pornographic content published or displayed on the service by means of- a) software or an automated tool or algorithm applied by the provider or by a person acting on behalf of the provider; or b) an automated tool or algorithm made available on the service by the provider or by a person acting on behalf of the provider."[85]
'Published or displayed'	Content in this context particularly includes references to pornographic content that is- a) "only visible or audible to users as a result of interacting with content that is blurred, distorted or obscured (for example, by clicking on such content), but only where the pornographic content is present on the service"; ▪ "embedded on the service"; and ▪ "generated on the service by means of an automated tool or algorithm in response to a prompt by a user and is only visible or audible to that user (no matter for how short a time.)"[86] It does not include pornographic content that - ▪ "appears in search results of a search service or a combined service";[87] or

[83]Section 226(8)-(9) of the Act.
[84] Section 226 (10)-(11) of the Act.
[85] Section 79(2) of the Act.
[86] Section 79(6)(a) of the Act.
[87] Section 79(6)(b) of the Act.

Term	Meaning
	▪ "is user-generated content in relation to that service."[88]
'Regulated provider pornographic content'	Provider pornographic content other than content that – a) "Consists only of text, or b) Consists only of text accompanied by – • A GIF which is not itself pornographic content; • An emoji or other symbol; or • A combination of (i) and (ii);[89] or • "Consists of a paid-for advertisement."[90]
'User-generated content'	Content that is "generated directly on the service by a user of the service or uploaded to or shared on the service by a user of the service" and, "that may be encountered by another user, or other users, of the service by means of the service."[91]

Additional terms used in this guidance

Term	Meaning
Access controls	Technical mechanism(s) which prevents users who have not been age assured, or having been age assured, did not meet the requirements of the age assurance process, from accessing a service (or part of it) or certain content.
Age assurance	Refers to both age verification and age estimation, as defined in section 230 of the Act. For these purposes, self-declaration of age is not considered to be a form of age assurance.
Age assurance method	Refers to the particular system or technology that underpins an age assurance process.
Age assurance process	Refers to the end-to-end process through which the age assurance method or combination of methods are implemented to determine whether or not a user is a child.

[88] Section 79(7) of the Act.
[89] Section 79(4) of the Act.
[90] Section 79(5) of the Act.
[91] Section 55(3) of the Act.