Social Media Minimum Age

Regulatory Guidance

September 2025

Australian Government

eSafety Commissioner

eSafety.gov.au

Contents

Introduction

The eSafety Commissioner (**eSafety**) has produced this guidance to assist providers of age-restricted social media platforms (**providers**) to meet their obligations as set out in Part 4A of the *Online Safety Act 2021* (Cth) (**the Act**). Separate resources about the social media minimum age (**SMMA**) obligation will be provided for young people, parents, educators and different community groups.

The Act does not prescribe how providers must comply with the SMMA obligation in s 63D, but it does provide for eSafety to formulate and promote guidelines for the taking of reasonable steps to prevent age-restricted users having accounts with age-restricted social media platforms.[1] **This regulatory guidance constitutes eSafety's guidelines**.[2]

Consistent with feedback obtained through stakeholder consultations and the approach of international regulators, eSafety has taken a principles-based approach to this guidance rather than being prescriptive. Accordingly, after setting out the underlying **legal, regulatory and technological context**, this guidance provides an explanation of **guiding principles** before setting out **guidelines on reasonable steps** to comply with the SMMA obligation. It then goes on to explain eSafety's **approach to compliance monitoring and enforcement**. The types of compliance information that providers should be recording and therefore capable of providing to eSafety are signalled throughout the guidance.

This guidance should be read alongside eSafety's other corporate documents, including our **self-assessment tool** to support services to assess whether they are providers and therefore subject to the SMMA obligation, eSafety's statement of **commitment to children's rights**, our **compliance and enforcement policy**, and eSafety's **regulatory guidance for other schemes** under the Act.

In the lead up to, and when the SMMA obligation takes effect on **10 December 2025**, eSafety expects providers' initial focus to be on the **detection and deactivation/removal of existing accounts** held by children under 16, including via **accessible pathways to report underage accounts**. We expect this to be accompanied by **clear and timely information** to those account holders about what will happen to their account, how they can download their information, where they can get support if they are feeling distressed, and how to challenge or seek review of the platform's determination that they are under 16, including through the use of age assurance measures. Providers are also expected to take reasonable

[1] Section 27(1)(qa)-(qb) of the Act.
[2] Section 27(qa)-(qb) of the Act.

steps to **prevent those whose accounts have been deactivated or removed from immediately creating a new account**.

However, eSafety also expects measures undertaken by providers will not be static. eSafety considers it reasonable that platforms will continuously seek to improve the reliability, robustness and effectiveness of their measures.

Independently of eSafety, the Office of the Australian Information Commissioner (**OAIC**) has an important role in monitoring and enforcing compliance with the privacy provisions set out in the Act, as well as those set out under the *Privacy Act 1988* (Cth) (**the Privacy Act**).

Disclaimer

This guidance **does not constitute legal advice**. Providers are responsible for conducting their own legal and privacy assessments, including consideration of their obligations under the Act, the Privacy Act, and any other applicable legislation or regulation.

Providers should seek and obtain independent legal advice in relation to their legal obligations and undertake privacy impact assessments tailored to their specific service(s), user base, and operational context.

eSafety reserves the right to amend or supplement this guidance at any time. **This guidance will be reviewed and updated by June 2026,** and periodically thereafter, to ensure it accounts for the dynamic technological and regulatory landscape and other relevant developments.

Key inputs to this guidance

Key inputs to this guidance include the Australian Government-sponsored Age Assurance Technology Trial (**the trial**), eSafety's stakeholder consultations, and eSafety's previous work relating to age assurance.

The Age Assurance Technology Trial

The trial report was published on **1 September 2025**.[3]

The trial was led by Age Check Certification Scheme (**ACCS**), an independent conformity assessment body for age assurance technologies based in the United Kingdom (**UK**), and funded by the Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts (**DITRDCSA**).

The trial examined **age verification**, **age estimation**, **age inference**, **parental control** and **consent**, and **technology stack** deployments in the Australian context for a range of purposes, including but not limited to reducing underage social media use.

The trial did not make policy recommendations or endorse specific types of age assurance, and it did not reflect a complete assessment of all relevant issues. Rather, it focused on assessing whether age assurance technologies are technically feasible and practically implementable. eSafety has drawn upon the concepts, definitions and findings of the trial report in developing this guidance.

Headline findings included that **age assurance can be done in Australia privately, efficiently, and effectively** – however, there is **no one-size-fits-all solution**. The trial also pointed out areas where guidance is needed from regulators, for example, on appropriate information for audits and demonstrating compliance. eSafety has sought to address those points in this guidance.

Providers are encouraged to consider the findings of the trial, which can help them to understand the technologies on offer in the current market. This includes their readiness for deployment in the Australian context, some of their strengths and weaknesses, opportunities for improvement and how they align with current and emerging international standards.[4] However, providers should make their own determination about which

[3] ACCS (2025), *Age Assurance Technology Trial – Report*, Department of Infrastructure, Regional Development, Communications, Sports and the Arts.

[4] For example, IEEE 2089.13, published in 2024, and the 27566 Series of International Standards relates to Information security, cybersecurity and privacy protection – Age Assurance Systems. Part 1 is the Framework document and is at Final Draft International Standard Stage.

method(s) or third-party vendor(s) they utilise. **Providers do not need to use methods or vendors included in the trial to be compliant with the SMMA obligation**, though there may be benefits to using systems and technologies which have been independently evaluated.[5]

More information is available at the trial website.

eSafety's stakeholder consultation

Between June and August 2025, **eSafety consulted with more than 345 people representing over 160 organisations** across the technology industry, academia, government, non-government sectors, and civil society. The consultation process focused on how eSafety implements its functions under the Act – not on the contents of the legislation itself, which has already been passed by Parliament. This included speaking directly with children and young people, as well as groups representing perspectives from parents and carers, Aboriginal and Torres Strait Islander people, people from culturally and linguistically diverse backgrounds, people with disability, people who identify as LGBTIQ+, people from regional and remote areas and older Australians.

A consultation survey was also sent to more than 150 people who had expressed an interest in providing their views. We received more than 35 responses to the survey.

This guidance draws on what consultation participants told us about the use of age assurance, the benefits and risks to different groups, possible circumvention tactics, unintended consequences, and how eSafety's guidance can seek to reduce these.

More information about the consultations is available on our website.

eSafety's previous work

eSafety has also drawn on our previous work in developing this guidance, including our 2023 Age Verification Roadmap and Background Report, our 2024 Age Assurance Trends and Challenges Issues Paper, and our 2025 Behind the Screen Transparency Report.

[5] For example, the ongoing evaluation by US National Institute of Standards and Technology (NIST) on Face Analysis Technology Evaluation (FATE) Age Estimation and Verification, or accreditation under the voluntary Accreditation Scheme for digital ID service providers in Australia's digital ID system.

Part 1: Legal, regulatory and technological context

In December 2024, the Parliament of Australia enacted the *Online Safety Amendment (Social Media Minimum Age) Act 2024*, introducing a new Part 4A into the Act.

Section 63D requires providers subject to these legislative obligations to take reasonable steps to prevent Australian children under 16 (**age-restricted users**) from having accounts on their platforms. Providers must comply from 10 December 2025.[6] The obligation applies to both **existing accounts** (those created before 10 December 2025) and **those created after 10 December 2025**.[7]

1.1 Who plays what role

There are distinct roles for the Minister for Communications, the Information Commissioner and eSafety in the implementation, oversight, and enforcement of the SMMA obligation.

The **Minister for Communications** may:

- Make legislative rules **specifying services that are or are not covered** by the definition of 'age-restricted social media platform'.[8] Before making any legislative rules of this type, the Minister must seek and have regard to advice from the eSafety Commissioner.[9]

  On 19 June 2025, in response to a formal request from the Minister, eSafety provided advice on draft legislative rules specifying services that are not age-restricted social platforms. On 29 July 2025, the Minister made the Online Safety (Age-Restricted Social Media Platforms) Rules 2025 (the Rules), specifying services that are not age-restricted social media platforms.

- Make any legislative rules **specifying kinds of information that providers of age-restricted social media platforms must not collect** for purposes of complying with the SMMA obligation.[10] Before making any legislative rules of this type, the Minister must seek and have regard to advice from the eSafety Commissioner and the Information Commissioner.[11] The Act already places restrictions on the use of certain

[6] Section 63E of the Act; Minister's instrument.
[7] Section 63E(4) of the Act.
[8] Section 63C(1)(b), 6(b) of the Act.
[9] Section 63(5)(a) of the Act.
[10] Section 63DA(1) of the Act.
[11] Section 63DA(2) of the Act.

identification material and significant penalties apply where those restrictions are not met. As at September 2025, no additional rules have been made.[12]

- **Specifying, by notifiable instrument, a day for the obligations to take effect**.[13] The Minister for Communications has made such an instrument and specified that the obligation will take effect on **10 December 2025**.
- **Initiating an independent review of the operation of the SMMA**.[14] This must be initiated within two years after the day the s 63D obligation takes effect.[15] This review will be managed by DITRDCSA. eSafety will conduct an ongoing evaluation of our implementation efforts, supported by an independent advisory panel.

The **Information Commissioner** is responsible for:

- **Providing advice to the Minister** on the kinds of information that must not be collected by age restricted social media platforms.
- **Functions under the Privacy Act** that are triggered if an 'interference with the privacy of an individual' occurs as defined in subsections 63F(1) and (3) of the Act.
- Preparing and publishing **platform provider notifications** if satisfied that an 'age restricted social media platform' has contravened subsection 63F(1) or (3) of the Act.
- **Making sure regulated entities follow the Privacy Act and other laws** when handling personal information, including sensitive information. This can involve conducting investigations and handling complaints.

eSafety is responsible for:

- Formulating and promoting **written guidelines for the taking of reasonable steps** to prevent age-restricted users having accounts with age-restricted social media platforms.[16]
- **Monitoring and enforcing compliance with the requirement to take reasonable steps to prevent age-restricted users having accounts.**[17]
- **Monitoring and enforcing compliance with the requirement to:**
    - not collect information where legislative rules are made specifying kinds of information that must not be collected[18]

[12] Section 63DB of the Act.
[13] Section 63E(2) of the Act.
[14] Section 239B of the Act.
[15] Section 239B(1) of the Act.
[16] Section 27(1)(qa)-(qb) of the Act.
[17] Section 63D, 63J of the Act.
[18] As of September 2025, no legislative rules have been made under section 63DA of the Act.

- not collect government-issued identification material or use an **accredited provider**[19] unless a reasonable alternative means is provided.

Providers may choose to offer the **option** to end-users to provide government-issued identification or use the services of an accredited provider. However, if a provider wants to employ an age assurance method that requires the collection of government-issued identification, then the provider **must** always offer a reasonable alternative that doesn't require the collection of government-issued identification.[20] A provider can **never require** an end-user to give government-issued identification as the sole method of age assurance and must always give end-users an alternative choice if one of the age assurance options is to use government-issued identification.[21] A provider also cannot implement an age assurance system which requires end-users to use the services of an accredited provider without providing the end-user with other choices.[22]

Reasonable alternative means may include, but are not limited to, end-user interaction with the service such as review processes (see Part 2.4.4).

Government-issued identification material[23] includes identification documents issued by the Commonwealth, a State or a Territory, or by an authority or agency of the Commonwealth, a State or a Territory (including copies of such documents).

A **digital ID** within the meaning of the Digital ID Act 2024 issued by the Commonwealth, a State or a Territory, or by an authority or agency of the Commonwealth, a State or a Territory. Providers are also prohibited from using an accredited service within the meaning of the Digital ID Act 2024 unless a reasonable alternative is provided.[24]

- **Monitoring and enforcing compliance with the Act more broadly:**
  - Providers may also have additional obligations under the Act and regulatory instruments regarding the use of age assurance and other methods to prevent access or exposure to certain content based on age. Compliance with similar obligations does not necessarily mean providers are compliant with the SMMA obligation. However, platforms may implement measures which meet multiple obligations. eSafety encourages platforms to carefully consider where obligations intersect and seek independent legal advice regarding their service

[19] *Digital ID Act 2024* (Cth).
[20] Section 63DB of the Act.
[21] Section 63DB of the Act.
[22] This is consistent with a fundamental principle of 'voluntariness' in the Digital ID framework.
[23] Section 63DB(4) of the Act.
[24] Section 63DB(1)(b) of the Act. Australia has two main regulators for its digital ID system – the Australian Competition and Consumer Commission (ACCC), which acts as the digital ID regulator for accreditation and compliance, and the OAIC, which oversees the privacy aspects of the system.

and compliance with all elements of Part 4A of the Act, relevant Industry Codes or Standards, the Basic Online Safety Expectations and other regulatory instruments. For more information, see eSafety's other regulatory guidance.

Part 3 of this guidance outlines eSafety' approach to compliance monitoring and enforcement, including our approach to deactivation and deletion of accounts and how we intend to use our information-gathering powers.

1.2 What is an 'age-restricted social media platform'?

An 'age-restricted social media platform' means an electronic service that satisfies the following conditions:[25]

- The **sole purpose**, or a significant purpose, of the service is to enable **online social interaction** between 2 or more end-users, *and*
- The service allows end-users to **link to, or interact with**, some or all of the other end-users, *and*
- The service allows end-users to **post material** on the service, *and*
- Such other conditions (if any) as are set out in the legislative rules.

The Minister for Communications may also specify in legislative rules that a particular electronic service is an age-restricted social media platform.[26]

An electronic service is **not** an 'age-restricted social media platform' if:[27]

- None of the material on the service is accessible to, or delivered to, one or more **end-users in Australia**, or
- The service is excluded in any legislative rules made by the Minister for Communications.

eSafety has released **separate guidance to support services to self-assess whether they are an age-restricted social media platform or excluded by the Rules**. See eSafety's self-assessment tool.

1.3 Approaches to determining location

Providers will need to consider and employ methods to determine whether an end-user is ordinarily resident in Australia to ensure that only children under the age of 16 who are

[25] Section 63C of the Act.
[26] Section 63C(4) of the Act.
[27] Section 63C(6) of the Act.

ordinarily resident in Australia are prevented from having an account on their service.[28] There are several ways this can be done by providers, including the use of location information.

1.3.1 Location information

An end-user's likely country of residency can be determined using a range of information which is available to services. For example, as part of the process of creating an account, an end-user may have provided information which is relevant to determining location such as an Australian mobile number. Some services may also collect and use information from end-users which can assist in determining whether an end-user is ordinarily resident in Australia, like IP address, GPS information, device language and time settings and device identifiers, as well as telephony information about the mobile service provider or carrier name.

Additionally, other information may be able to be obtained such as information from app stores or operating systems and account settings which indicate a person is ordinarily resident in Australia. End-users may also provide or share information that is available to the service in the course of using the service, such as photos, tags, connections, engagement and other activity indicating they are ordinarily resident in Australia.[29]

Providers can determine an end-user's likely country of residence based on a combination of digital signals, many of which are already shared by users.[30] Systems typically aggregate multiple data points, including but not limited to, an end-user's IP address, GPS signals, Wi-Fi network information, mobile phone tower connections and device and browser fingerprinting.

It is commonly used for a range of purposes such as offering location-specific services (for example, emergency services alerts) or ensuring legal compliance (for example, in gambling contexts). Some social media platforms use location data to provide personalised recommendations, including ads, or detect suspicious or fraudulent activity.

Considerations for SMMA

Location information can help determine if an end-user is ordinarily physically present in Australia and therefore may be an indication that an end-user is ordinarily resident in Australia. It can also be used to provide additional information on whether an end-user is

[28] eSafety would not expect providers to take action on accounts holders who are not ordinarily resident in Australia, such as those temporarily visiting Australia.
[29] In some circumstances, location information may be personal information. Office of the Australian Information Commissioner (OAIC) (2022), Chapter B: Key concepts, OAIC website.
[30] ACCS (2025), *Age Assurance Technology Trial – Report*, Part J 15.5.

in Australia if they are connecting via a VPN. The trial found that such tools are in place in Australia for other purposes.[31]

1.4 Age assurance

Providers will need to consider and employ age assurance methods to comply with the SMMA obligation.[32] This section provides a broad overview of the different types of age assurance measures and the different considerations providers should have regard to when deploying these to comply with the SMMA obligation. As noted above, eSafety will take a principles-based approach to assessing compliance with the SMMA obligation and **does not require specific types of age assurance to be employed**.

Part 2 of this document includes guidance to providers on how age assurance may be used to detect accounts belonging to age-restricted users and to prevent age-restricted users from having accounts.

1.4.1 What is age assurance?

Age assurance is a broad term that refers to a range of processes and methods used to verify, estimate or infer a person's age or age range.[33]

Appropriate and proportionate implementation of age assurance, bolstered by a range of complementary measures, can create safe and age-appropriate experiences online.[34] Whether the use of age assurance is reasonable for purposes of the SMMA obligation will depend on both the **age assurance method(s)** used and the **systems and processes** surrounding these method(s).

The risks, benefits, level of certainty, and other considerations regarding use of an age assurance method depend on the technology underlying the method itself, the circumstances in which it is used, how it is implemented, and how the systems around it are designed and deployed.

---

[31] For example, Stan and Kayo Sports use commercial geo-location tools for real-time VPN detection. These tools check the origin of IP addresses, DNS requests and device fingerprints to identify if a user is masking their location; ACCS (2025), *Age Assurance Technology Trial – Report*, Part J.15.20.

[32] Explanatory Memorandum (EM), *Online Safety Amendment (Social Media Minimum Age) Bill* 2024 (Cth), p. 21. *Section 63D of the Act does not prescribe what 'reasonable steps' platforms must take. However, it is expected that at a minimum, the obligation will require platforms to implement some form of age assurance, as a means of identifying whether a prospective or existing account holder is an Australian child under the age of 16 years.*

[33] ISO FDIS 27566-1 – Information security, cybersecurity and privacy protection - Age assurance systems – Age assurance is a set of processes and methods used to verify, estimate or infer the age or age range of an individual, enabling organisations to make age-related eligibility decisions with varying degrees of certainty.

[34] eSafety Commissioner (2024), *Age Assurance - Issues paper*, eSafety website. Appropriate age assurance measures are an element of other schemes including the Basic Online Safety Expectations and Industry Codes and Standards.

Terminology[35]

Age assurance systems refer to systems that use one or more **age assurance methods** to provide a relying party with the necessary information to make an **age-related eligibility decision**.

Age assurance method means the technology or process used to establish an age assurance result (information indicating that a person is a certain age, over or under a certain age or within a certain age range).

Age assurance methods include:

- **Age estimation** methods: analysis of biological or behavioural features of humans that vary with age.
- **Age inference** methods: uses information, other than a date of birth, which indirectly implies that an individual is over or under a certain age or within an age range.
- **Age verification** methods: calculating the difference between a verified year or date of birth of an individual and a subsequent date.

Each of these age assurance methods was assessed in the trial. Providers are encouraged to consider the findings of the trial, which can help them understand the technologies on offer in the current market, their readiness for deployment in the Australian context, some of their strengths and weaknesses, and opportunities for improvement. However, providers should make their own determination about which method(s) or third-party vendor(s) they use.

The sections below briefly discuss each of these methods in the context of the SMMA.

1.4.2 Age estimation

This method uses statistical models to estimate the likely age of an end-user based on observable characteristics such as facial features, voice or behavioural patterns.[36]

The trial found **age estimation is technically feasible and already in use** across sectors such as social media, retail, and age-restricted content providers.

---

[35] This terminology is aligned with the trial, as well as ISO FDIS 27566-1 – Information security, cybersecurity and privacy protection - Age assurance systems, the draft international standard currently under development by the International Organisation for Standardisation (ISO) to establish core principles for enabling age-related eligibility decisions.

[36] ACCS (2025), *Age Assurance Technology Trial – Report*, Part D.2.1.

Considerations for SMMA

The trial noted that the **accuracy of tested methods drops near legal thresholds**, due to natural error margins and demographic variability. While demographic fairness is improving, the trial noted ongoing challenges, particularly for end-users with darker skin tones and those aged 16–20.

The trial report outlined the role of **buffer thresholds**, to account for the uncertainty around threshold ages. For example, at a threshold of 18, a service may accept those who are estimated to be 21+, reject those estimated to be under 15 (as the confidence that they are over/under 18 is high) and require additional checks for those estimated to be in the range of 15-21 (the **buffer zone**), where there is lower confidence in the estimation result for over/under 18. For SMMA, this approach may help minimise **false positives** in the form of an end-user under 16 being positively identified as over 16 and as a result being erroneously approved to have an account. However, the approach may also result in **over-blocking** of eligible end-users aged 16 and over. This highlights the need for **careful configuration and fallback mechanisms within age assurance systems** and providing options and review pathways for end-users.

1.4.3 Age inference

Age inference draws probabilistic conclusions about facts other than a date of birth to imply a likely age or range. The conclusions can be based on behavioural patterns, contextual data, digital interactions, metadata or a range of other information.

Age inference methods ranged in maturity and were not tested in standalone trials but formed part of broader system evaluations.

The trial found **age inference is technically feasible in Australia**, with no substantial limitations to its implementation.

Considerations for SMMA

As with age estimation, age inference results near thresholds are generally less precise than age verification. When making decisions based on age inference results, providers should take care to ensure there is a logical and evidence-based connection between the inference and the age result, noting different data points have different weighting for reliability. This may help avoid misclassifying end-users with atypical behaviours or interests.

Providers should also carefully consider the impact on end-user privacy and whether it is proportionate in the circumstances, particularly in regard to end-user expectations, data minimisation, and the sensitivity of personal information handled to inform inference

results. Providers should be prepared to report on the range of personal information being collected and used for this method. This should include the type and amount of information necessary and the frequency and timing of collection and use required to operate effective inference methods.

Systems in the trial commonly used conservative buffer thresholds near critical age thresholds, including 16, and often escalated end-users to age estimation or verification methods when the confidence in the inference was low. As reflected above, buffer zones should be carefully calibrated to prevent unreasonable restrictions on end-users.

1.4.4 Age verification

Age verification is considered a technically mature, **high-certainty and low-ambiguity** method of determining an age assurance result.[37] It relies on validating an authoritative source of a person's date of birth compared with the current date, which can allow for a precise age result if required. It is already in use across various regulated industries.[38]

Considerations for SMMA

Systems that only accept government ID as the authoritative source for an end-user's date of birth, such as some document-based services, **cannot** be relied on by providers as the sole option for end-users.[39] Providers must always provide **reasonable alternative means**, which may include some of the other methods outlined in this guidance. **Providers are not required to age verify all their end-users to meet their reasonable steps obligations**.

1.4.5 In-house or third-party age assurance

A provider of an age-restricted social media platform may rely on a contracted third-party vendor as an alternative, or to supplement 'in-house' or 'proprietary' systems for age assurance to support assessing whether an end-user is an age-restricted user.

In addition to those age assurance results, providers may also consider other age signals or information, such as from other services in the **technology stack or** across a digital ecosystem, when making **age-based eligibility decisions**.[40]

---

[37] ACCS (2025), *Age Assurance Technology Trial – Report*, Part C.2.1.
[38] For example, same-day alcohol delivery: Liquor & Gaming NSW (2024) Same say delivery age verification requirements.
[39] Section 63DB of the Act.
[40] This could include age information or signals from app stores, devices, parental controls and other sources if available.

Considerations for SMMA

Regardless of whether age assurance is in-house or third-party and where age assurance occurs in the technology stack, digital ecosystem, or user journey – **the obligation to take reasonable steps is on the provider of the age-restricted social media platform**. It is for the provider to determine whether the information available gives the provider sufficient confidence to determine whether an end-user is likely to be an age-restricted user and whether use of this information supports effective age assurance on their service to prevent under 16s from having an active account.

It is a matter for providers to determine whether to use a third-party vendor as part of their compliance with the SMMA obligation. Providers should ensure they have conducted **due diligence** on any third-party vendors they use to comply with the SMMA obligation to ensure their practices and the way they integrate with the platform reflect the principles and expectations outlined in this guidance. For example, providers should consider the availability of independent accreditation and/or evaluation and the potential exacerbation of scam risks for end-users.[41]

1.4.6 Successive validation

Successive validation uses multiple independent age assurance methods sequentially to establish an age assurance result. This is sometimes called a **waterfall approach** and can support providers in making more risk-appropriate decisions across the user journey. Successive validation may involve progressing through to age assurance methods that have higher certainty or specificity or may involve successive validation through a range of methods that create cumulative confidence.

The trial indicated **successive validation is both technically viable and operationally effective**. It describes successive validation as a design principle, not necessarily a product, which recognises that no single method works perfectly for all end-users, in all contexts, at all times.[42]

Considerations for SMMA

eSafety encourages providers to take a successive validation approach to support compliance with the SMMA obligation, enabling many providers to build on their existing systems and processes as set out in eSafety's February 2025 *Behind the Screen* report. The

[41] eSafety Commissioner (2025), *eSafety's consultation on the social media age restrictions* [PDF, 331.15 KB], eSafety website, p. 6. eSafety Commissioner (2025), *eSafety's consultation on the social media age restrictions* [PDF, 331.15 KB], eSafety website, p. 20; eSafety Commissioner (2025), *Social media minimum age obligations, roundtable discussion: Parents and carers* [PDF, 203 KB], pp. 11-12. eSafety website.
[42] ACCS (2025), *Age Assurance Technology Trial – Report*, Part F 7.7.

trial found that when implemented transparently and in line with privacy and security best practices, applying the design principle of successive validation has the potential to support inclusive, proportionate and scalable age assurance.[43]

eSafety will **not** dictate what age assurance or other steps are expected at **each stage of the user journey** (for example, at account creation or sign-up stage). However, providers **must not** collect government-issued identification material or use an accredited service[44] without providing reasonable alternative means for age assurance.[45]

eSafety expects providers to institute and monitor improvements to current practices and enforcement of existing approaches, as research including the *Behind the Screen* report has shown platforms have generally not been very effective at enforcing their minimum age rules to date, even where they have deployed age assurance systems and technologies.

1.5 Other related measures

Beyond the methods of age assurance categorised in the draft ISO standard for age assurance systems (ISO/IEC FDIS 27566-1), there are other related measures and processes that providers may consider – for example in layered or combined approaches to age assurance, or as part of broader age assurance systems.

- **Self-declaration:** a method where an end-user enters their own date of birth or age.
- **Vouching:** a method used to confirm a person's age where a trusted entity with an existing relationship to the person vouches for that person.[46]
- **Parental attestation or consent:** a mechanism that enables a parent or legal guardian to provide or revoke permission for a child.[47]
- **Parental controls:** a set of tools or settings that allow parents or guardians to manage, restrict or monitor a child's access to digital content, services or device functions.[48]
- **Interoperable models:** where different systems have the capacity to transfer trusted age signals or credentials across platforms, services or devices without re-verifying the end-user.

---

[43] ACCS (2025), *Age Assurance Technology Trial – Report*, DITRDCSA, Part F.2.8 and F 7.7.
[44] Within the meaning of the *Digital ID Act 2024* (Cth).
[45] Section 63DB of the Act.
[46] Age Verification Providers Association, How do you check age online?, AVPA website; eSafety (2023) Age verification background report.
[47] Parental consent was treated in the trial as a distinct functional model that flows from – but is not itself – a form of age assurance.
[48] ACCS (2025), *Age Assurance Technology Trial – Report*, Part G.4.1.

Considerations for SMMA

Age gates and self-declaration are generally not seen as sufficient for regulated contexts when used in isolation.[49] Accordingly, **eSafety does not consider the use of self-declaration, on its own without supporting validation mechanisms, to be reasonable for purposes of complying with the SMMA obligation**.

Vouching and parental attestation rely on the intention and understanding of the parent or person providing the vouching statement. There are risks that the person attesting to someone's age may not have the authority or information to do so or may assist circumvention by entering a false age.[50] Therefore, **eSafety does not consider vouching or attestation, on its own, without appropriate validity checks, to be reasonable for the purposes of complying with the SMMA obligation**. While vouching requires end-users to have access to a person able to provide a valid and reliable vouching statement, it does not require the end-user to have any specific documents or records and may be suitable for end-users who cannot engage with other age verification or estimation methods.

If implemented as part of broader age assurance systems, or combined with other evidence, providers should consider the circumstances in which vouching is appropriate and proportionate to risk, who can provide a vouching statement (for example, people in authority positions in a community) and what information is needed to establish its strength or validity.

Parental controls can play a role in managing a child's access to age restricted content and may be a possible source of indirect age signals.[51] Signals from the use of parental controls may suggest that an end-user is a child – for example, if an end-user attempts to sign up to a service on a device which has parental controls enabled. However, the reliability of these signals for establishing an end-user is **not** an age-restricted user is limited because they rely on parents or guardians entering a child's age and they may misrepresent this for a range of reasons.[52]

The trial found that **interoperable systems** are emerging but remain non-standardised. Many of these systems propose approaches where an age credential or token, based on a choice of age assurance methods, is stored in a way that an end-user can choose to reuse

---

[49] Ofcom in their *Guidance on highly effective age assurance – For Part 3 services* [PDF, 394 KB] and the European Commission in their *Research report: Mapping age assurance typologies and requirements* [PDF, 1.14 MB], have indicated that self-declaration alone is not considered an appropriate or highly effective method for age assurance. 5Rights in their *But how do they know it is a child – Age Assurance in the Digital World Report* [PDF, 706 KB] has suggested it may be appropriate for low-risk products and services that do not include features that impact negatively on children.

[50] eSafety Commissioner (2025), *Behind the screen: The reality of age assurance and social media access for young Australians – Transparency report*, eSafety Commissioner.

[51] ACCS (2025), *Age Assurance Technology Trial – Report*, Part G.4.3.

[52] ACCS (2025), *Age Assurance Technology Trial – Report*, Part G.4.5.

that check for multiple services or access requests. These methods vary in their architectural model, credential type, data sharing protocol and trust management approaches.

Providers are encouraged to consider approaches that decrease end-user burden and enable control over personal information. **Whether the reliance on age information shared through interoperable systems is reasonable will depend on the circumstances, strength and robustness of the signals available.**

Part 2: Reasonable steps guidelines

2.1 Overview

eSafety acknowledges there is no one set of measures suitable for all end-users, platforms or circumstances. What is reasonable will be contextually dependent with consideration given to the regulatory landscape, technological feasibility, the circumstances of the provider and the intention of the SMMA obligation – which is to reduce harm to age-restricted users. **There is no one-size fits all approach for what constitutes the taking of reasonable steps.**

Accordingly, while this document provides guidance and examples to assist providers, providers are required to make their own determination of what steps to take, and, if asked, to **demonstrate to eSafety that those steps were reasonable** in the circumstances. Providers should continuously evaluate and seek to improve their approach over time.

When taking reasonable steps to prevent age-restricted users from holding accounts, providers should consider and apply the **guiding principles** outlined in Part 2.2 of this document.

Broadly speaking, reasonable steps consist of **systems, technologies, people, processes, policies and communications** that support compliance with the SMMA obligation. The guidelines discuss each of those elements, with a particular focus on the use of **age assurance**.[53]

eSafety considers it is reasonable for platforms to take a layered approach across the user journey and implement a range of measures to meet the SMMA obligation.

This includes taking reasonable steps to:

- determine which accounts are held by age-restricted users and deactivate or remove those accounts with kindness, care and clear communication
- prevent age-restricted users from creating new accounts[54]
- mitigate circumvention of measures.

---

[53] '[I]t is expected that at a minimum, the obligation will require platforms to implement some form of age assurance, as a means of identifying whether a prospective or existing account holder is an Australian child under the age of 16 years.'
EM, *Online Safety Amendment (Social Media Minimum Age) Bill* 2024 (Cth) p. 3.

[54] Or for those users that deactivated their account when the SMMA obligation came into effect, from re-activating their account before they turn 16.

These steps are critical to ensuring age-restricted users cannot create, obtain or hold accounts on platforms.

eSafety considers the following **would not constitute reasonable steps** as their effect would be inconsistent with the objectives of the SMMA:

- Implementation that **relies entirely on self-declaration** to determine the age of existing or prospective account holders
- Implementation where measures rely on age-restricted users holding an account for an **unreasonable period of time before detection**. Measures that require end-users to engage with a platform for an extended period of time, including to collect sufficient data to assess their age, would allow age-restricted users to be exposed to the harms that the SMMA seeks to address.[55] What is reasonable will depend on the nature of the platform and other verification measures the platform has implemented as part of any layering approach
- Implementation where measures do not reasonably **prevent age-restricted users who have accounts deactivated or removed from immediately reactivating or creating a new account** and regaining access to the age-restricted social media platform
- Implementation of measures that result in substantial numbers of **end-users who are not age-restricted users, being removed or blocked from accessing services**.[56]

As these are non-exhaustive examples, there may be other instances where eSafety considers the steps taken by a platform do not constitute reasonable steps. As set out in the Explanatory Memorandum, what is reasonable will be:

> 'determined objectively, having regard to the suite of methods available, their relative effectiveness, costs associated with their implementation, and data and privacy implications on users, amongst other things.'[57]

Providers are encouraged to proactively engage with eSafety to voluntarily provide regular updates and information on how they intend to comply with the SMMA obligations.

---

[55] This could include self-declaration-based age-gates or certain age inference measures. These measures, however, may be useful for platforms in reducing the risk of age restricted users holding an account when layered with other measures and will be relevant when considering whether the platform took reasonable steps.
[56] This may be mitigated through effective and timely review mechanisms. See also Part 2.4.4. As noted below, providers should consider the proportionality of measures they implement, for example, requiring **all** users to undertake age verification and establish their age to a very high certainty is **not necessary for compliance**.
[57] EM, *Online Safety Amendment (Social Media Minimum Age) Bill* 2024 (Cth) p 3.

2.2 Guiding principles

Drawing on the trial, eSafety's consultations, our previous work – including the Age Verification Roadmap,[58] international regulatory approaches,[59] human rights expectations,[60] and eSafety's own commitments to child rights[61]– eSafety has identified the following principles that should inform providers' reasonable steps to comply with Part 4A of the Act.

The steps taken by providers should be:

- **Reliable, accurate, robust and effective**
- **Privacy-preserving and data-minimising**
- **Accessible, inclusive and fair**
- **Transparent**
- **Proportionate**
- **Evidence-based and responsive to emerging technology and risk**

Respect and protection of fundamental human rights – including the right to privacy, the right to equality and non-discrimination, freedom of expression, access to information, and the rights of the child – underpin all the guiding principles and should be front of mind for providers when implementing measures to meet the obligation.

More broadly, providers should have regard to the best interests and rights of children and young people in the design and operation of their services. The SMMA obligation does not negate the need for providers to consider the impact of their service design on children.

Having engaged and consulted with various stakeholders including children and young people, eSafety recognises that there is a strong preference for existing end-users that are under the age of 16 to be given a choice about what happens to their account, including the option to have their access suspended with their data retained by the platform, rather than removed so the end-user can resume using the account when they reach the age of 16 if they so choose. In support of existing end-users that are under the age of 16 being given a choice, eSafety's focus will be on the steps taken by providers to prevent existing

[58] eSafety Commissioner (2023) *Age verification consultation*, eSafety website.
[59] Ofcom (2025), *Guidance on highly effective age assurance – For Part 3 services* [394 KB], Ofcom website. European Commission (2025) *Guidelines on measures to ensure a high level of privacy, safety and security for minors online*, European Commission website; Information Commissioner's Office (ICO) (2024), *Joint Statement on a Common International Approach to Age Assurance*, ICO website; eSafety Commissioner (2025), *The Global Online Safety Regulators Network*, eSafety website.
[60] eSafety Commissioner (2025), *The Global Online Safety Regulators Network*, eSafety website.
[61] eSafety Commissioner (2024), *eSafety and the EU Child Rights Intergroup team up to protect children online*, eSafety website.

age-restricted users, at the time the SMMA comes into effect, from having **active** accounts and preventing those under 16 from **creating new** accounts.

Providers are encouraged to consider undertaking child rights impact assessments.[62] See eSafety's Statement of Commitment to Children's Rights in the implementation of the SMMA.

2.3 Applying the guiding principles to reasonable steps

2.3.1 Reliable, accurate, robust and effective

Providers should ensure age assurance measures – and the systems and processes surrounding them – are **reliable, accurate, robust and effective** to prevent age-restricted users from having accounts, while minimising the risk of accounts held by persons who are not age-restricted users being deactivated or removed.

Providers are encouraged to consider methods of age assurance that have been independently certified or accredited against relevant international and domestic standards on matters such as accuracy, security and fraud resilience.[63]

Reliability and accuracy

In the context of age assurance, systems should reliably produce a result that provides a provider with a sufficient level of confidence as to whether an end-user is an age-restricted user.

To enable a flexible and proportionate approach, **eSafety does not propose a minimum accuracy level** for age assurance methods. Platforms should determine if the measures or combination of measures implemented gives them sufficient confidence to make an **age-based eligibility decision** – including allowing account creation, deactivation/removal, or other action.

- Providers should **define acceptable error thresholds based on their risk, service type, and user base**. Providers are encouraged to consider relevant international standards and accreditation schemes to inform their consideration of accuracy levels.

---

[62] Providers should also consider relevant international standards, such as IEEE 2089-2021 IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children, codes of practice, such as the 5Rights AI Code, toolkits such as 5Rights Child Online Safety Toolkit and Assessing child rights impacts in relation to the digital environment | UNICEF Child Rights and Business, and guidance such as Child Rights Impact Assessments (CRIAs) to Support Youth Online - Cyberbullying Research Center.

[63] For example, ISO/IEC 27001 Information security, cybersecurity and privacy protection – Information security management systems - Requirements and ISO/IEC 30107 Information technology – Biometric presentation attack detection Part 1: Framework.

- Providers are not required to eliminate all uncertainty but should seek to minimise harm and ensure decisions are proportionate, fair, and reviewable. This includes the ability to report on error rates and work to continuously improve age assurance methods.

Where age assurance is based on inference or estimation and a **buffer threshold** is set, providers should ensure that the threshold is appropriately configured, having considered the accuracy of the underlying technology, the confidence of the estimation or inference, and the risk of unreasonably over-blocking users that are not age-restricted users. All age assurance methods should be backed by accessible, timely and accurate review processes.

Factors such as the provider's audience and demographics, other policies and practices, and risk profile are relevant considerations. In the case of **services tailored to more adult experiences**, such as dating apps or those that allow or promote adult content and experiences, eSafety considers it **reasonable for those types of services to set an age of 18+ in their terms of use and age assurance systems.**

Robustness

Providers should implement age assurance systems that are secure and reasonably resistant to circumvention, and ensure their own systems and processes are also sufficiently robust to withstand such challenges.

- Providers should **mitigate known and reasonably foreseeable circumvention risks**, with a particular focus where these are known to be accessible to children. Providers should consider technical and policy measures to address these risks.[64]
- Providers should ensure any age assurance method employed has undergone sufficient testing and evaluation before use and while in use. Providers are encouraged to **undertake and document ongoing internal testing procedures as well as seek external audits or independently validated testing** to support transparency.

Examples of measures platforms can take include:

- Conducting periodic **red-team testing**,[65] including simulating bypass attempts by underage end-users

[64] For example, liveness detection where an age assurance method requires facial imagery or responding and investigating where account behaviour patterns suggest an account has been transferred to an age-restricted user. See discussion at 2.5.3 for further guidance.

[65] Testing to see if something can be circumvented, bypassed or tricked. A red team is a group of people authorised and organised to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. National Institute of Standards and Technology (NIST) (2025), *Information Technology Labatory Computer Security Resource Center – Glossary,* NIST website.

- Procuring **third-party audits**[66] of age assurance and complementary measures, including circumvention controls.

Providers should ensure that review and evaluation are conducted regularly and in response to any material changes on the platform. Evaluation criteria, outcomes, and processes should be recorded to demonstrate they have taken reasonable steps and be provided to eSafety.

Effectiveness

All measures, including age assurance measures, have different risks and benefits. eSafety also acknowledges that no measure, whether technological or policy based, is completely effective in all scenarios.

Providers should be able to demonstrate that the combination of steps they have taken is **cumulatively effective in preventing age-restricted users from having accounts and limiting the associated harms**.

Providers should determine, record, and be prepared to report to eSafety on their effectiveness and impact metrics. These metrics should be periodically reviewed. Relevant metrics and indicators may include numbers of account removals, subsequent reviews sought and undertaken, effectiveness (error/success rates) of various internal age assurance measures, the outputs of third-party audits and user reports. eSafety also encourages providers to make the results of reviews and audits available to the public where possible.

2.3.2 Privacy-preserving and data-minimising

Privacy and the protection of personal information are important for everyone's agency, dignity, and safety.[67]

Steps to comply with the SMMA obligation **will not be reasonable unless** providers also comply with their information[68] and privacy[69] obligations under Part 4A of the Act, as well as the Privacy Act and the Australian Privacy Principles regulated by the OAIC.

This means providers must comply with Privacy Act obligations when using existing personal information for the secondary purpose of taking reasonable steps to prevent age-

[66] An assessment conducted by an independent, external entity.
[67] Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation, and that everyone has the right to the protection of the law against such interference or attacks. For interference with privacy not to be arbitrary, it must be lawful and in accordance with the provisions, aims and objective of the ICCPR and should be reasonable in the particular circumstances.
[68] Section 63DA and 63DB of the Act.
[69] Section 63F of the Act.

restricted users having accounts. eSafety considers that once obligations under s63F are met, obligations under the Privacy Act continue to apply for any subsequent collection and use.

Providers should also have regard to any privacy and related guidance released by the OAIC.

Providers should assess the minimum information and data needed to make decisions appropriate for their service and circumstances. Policies should be calibrated to ensure the collection, use and retention of personal information is reasonably necessary and proportionate. Providers are strongly encouraged to use non-personal information as far as possible, and avoid handling of **sensitive personal information**.[70]

eSafety **does not expect providers to retain personal information as a record of individual age checks.** See Part 3.1.2 for more information about the types of data, indicators and metrics that eSafety may require to assess compliance.

2.3.3 Accessible, inclusive and fair

Providers should ensure age assurance methods and surrounding systems and processes are accessible, inclusive and fair.

To achieve this, eSafety expects providers to consider the range of existing and prospective Australian end-users with **diversity in appearance, abilities and capacities**, and implement systems and safeguards to ensure their methods are accessible and produce outcomes that are inclusive and fair for all end-users.

The use of age assurance should not unfairly inhibit access for certain end-users or impact certain groups disproportionately without adequate mitigations and support to minimise the potential for bias and discrimination.

- Providers should test their age assurance methods in the Australian context, including by looking at **different demographics within Australia** and whether the age assurance system is accessible, inclusive and fair for these demographics. Accuracy should be evaluated and recorded across different cohorts, with an aim to minimise bias and improve consistency in results over time.
- Providers should **mitigate the impact of accessibility or bias issues** in the age assurance methods they use and **build processes to support those who may be adversely affected**. This includes ensuring that systems are inclusive of the diverse needs of communities across Australia — such as Aboriginal and Torres Strait

[70] Office of the Australian Information Commissioner (OAIC) (2022), Chapter B: Key concepts, OAIC website.

Islander peoples, culturally and linguistically diverse communities, and those with limited access to digital infrastructure or identity documentation. This is particularly relevant where age assurance methods are based on machine learning or involve automated decision making.

End-users should be able to understand age assurance systems.

- Providers should produce **clear and easy-to-understand information** about their age assurance methods. This information should be made available for users at a range of literacy levels and in a variety of different languages. In developing this information, providers should also ensure alignment with Web Content Accessibility Guidelines (WCAG) 2.1.

Age assurance methods should be adaptable to individual end-user circumstances, needs and preferences.

- Providers should offer a **choice** between a range of age assurance methods, giving end-users flexibility and agency in choosing methods that best suit their circumstances.
- Providers should account for those who do not have access to documents, are facing challenging circumstances or experiencing vulnerability, or otherwise **face barriers** engaging with age assurance methods. This should include accepting a range of options rather than a narrow list of age documents and providing non-document-based options.
- Where appropriate, providers may consider methods such as professional or community vouching, or assessment of alternative evidence of age, where end-users have been unable or unwilling to use other provided methods of age assurance. Providers should consider whether this is reasonable in the circumstances and ensure such methods are supported by appropriate validity checks.

2.3.4 Transparent

Reasonable steps, including age assurance methods and surrounding systems and processes, should be transparent and clear to end-users.

Information about providers' use of age assurance and other measures should use age-appropriate language and be accessible to people of different literacy levels and abilities. It should include:

- plain-language explanations of **when and why age assurance is required**
- guidance on **what age assurance options** are being used or are available to users

- what **personal information** will be collected, used, how it will be stored and protected, possible outcomes, and what the provider will do with the result – including what is retained or destroyed and what other privacy protections are in place and relevant transparency obligations under the Privacy Act
- information about **what is happening or may happen to age-restricted users' accounts**, how they can download their information, the basis of and right to seek review of any decision, and where they can go for support (as discussed in more detail in Part 2.5.2).

Providers should be able to report on the uptake of their support resources, make them easy to access for all end-users and promote their availability to the public.

Transparency measures are also key to building trust and addressing the community's concerns about age assurance. eSafety understands that there is low public awareness among both Australian adults and children of the range of age assurance technologies available, including those currently in use, and how they work in practice.[71] Participants in the consumer research commissioned by DITRDCSA, also reported low trust in platforms and held concerns about the privacy and security of their information, which can result in a lower willingness to engage with certain age assurance measures.[72]

Reducing scams and phishing through transparency

Providers should clearly communicate what legitimate age assurance looks like – such as through use of official branding, secure URLs, and explaining on the provider's service whether end-users will be directed to a third-party vendor, and the steps they will have to take or information they will have to provide, to reduce end-user susceptibility to scams.

Sharing information can help disrupt scams faster and reduce associated harms. If a provider becomes aware that their age assurance process is being routinely compromised, it should take steps to proactively inform the public.[73]

2.3.5 Proportionate

Proportionality and consideration of risk and harm are key components of determining what constitutes reasonable steps. Providers should consider the balance of the measures

[71] DITRDCSA (2025), *Age assurance consumer research findings*, DITRDCSA website, p. 22.
[72] DITRDCSA (2025), *Age assurance consumer research findings*, DITRDCSA website, p 39.
[73] Providers are also encouraged to engage with the National Anti-Scam Centre. This is a virtual centre that sits within the ACCC and brings together experts from government, law enforcement and the private sector, to disrupt scams before they reach consumers. See more at the National Anti-Scam Centre website. Scamwatch collects reports about scams to help us warn others and to take action to stop scams. It also provides up-to-date information to help consumers spot and avoid scams.

they implement having regard to their purpose, the risk of harm they mitigate and the impact they have on end-users.

Risk

What constitutes reasonable steps will depend on the risk profile of the service. Services may have a higher risk profile where they have comparatively higher:

- existing numbers of children and young people holding accounts
- prevalence of features associated with harm to children and young people (such as algorithmic content recommendation, 'likes', persistent notifications and endless scroll)[74]
- prevalence of content associated with harm to children and young people (such as violent material and material that promotes unsafe eating habits.)[75]

Providers of a service with a **higher risk profile are expected to employ more robust measures** to prevent age-restricted users from having an account.

Layering different measures and levels of assurance

Employing a range of tools, including different methods for age assurance, tailored for different risks and based on the circumstances can support a proportionate implementation of age assurance.

When layering methods, providers should consider the reasonable level of confidence needed to determine whether to act[76] on an account, and the impact or friction of an age assurance measure and the total impact of the measures implemented by a service or within a system.

Impacts on users

Providers should avoid **unreasonable practices that risk over-blocking access or infringing on the rights of Australians**. For example, requiring **all** existing Australian account holders to prove their age using an age verification system may be unreasonable and is not necessary for compliance – particularly in circumstances where the provider could use existing data to infer with reasonable confidence that certain end-users are over 16.[77]

---

[74] Explanatory Statement, *Online Safety (Age-Restricted Socia Media Platforms) Rules* 2025 (Cth), p 1.
[75] EM, *Online Safety Amendment (Social Media Minimum Age) Bill* 2024 (Cth), p. 16 and 21. Some of this content may also be regulated by other regulatory schemes under the Act, for example, the Phase 2 Industry Codes.
[76] For example, taking investigatory actions, asking users for more information or to go through age assurance measures, and deleting or deactivating accounts.
[77] For example, the length of time an account has been held. See also, parts 1.4.3 and 2.4.1 of this guidance and Part E – Age Inference of *Age Assurance Technology Trial – Report*.

Providers should consider and document risk assessments to demonstrate the measures taken, including age assurance measures, are proportionate to the risk.

2.3.6 Evidence-based and responsive to emerging technology and risks

Changes in platform features and functionalities, as well as shifts in end-user behaviour and patterns over time, carry associated risks and contribute to an ecosystem that requires ongoing adaptability. What may be considered reasonable today could quickly become inadequate as the environment changes, whether due to emerging risks, changes to platforms or advancements in technology.

eSafety expects measures taken by providers will not be static. Providers should proactively monitor and respond to changes in their platforms' features, functions, and end-user practices, particularly where these or other changes may introduce new risks. eSafety considers it reasonable that platforms be prepared to demonstrate they are continuously monitoring, uplifting and seeking to improve the reliability, robustness and effectiveness of their measures over time. This includes maintaining awareness of:

- **changes in circumvention methods** and associated risks – for example, where generative AI may be used for fraudulent documents or to attempt to bypass facial age estimation
- **changes in end-user behaviour and demographics**, including where children and young people **migrate to different services** where they experience different risks and harms. In this instance any insights should be provided to eSafety
- community expectations of privacy
- **scams, privacy complaints and data breaches** that may emerge in response to increased uptake of age assurance
- **new developments in age assurance**. Providers should regularly review their measures and update them where appropriate, especially where new approaches better support the guiding principles and the aim of SMMA. For example:
- Exploring new and emerging methods that are more privacy preserving or require less end-user data
- Considering interoperable options, digital wallet integrations and zero-knowledge proof methods, that decrease end-user burden and enable control over personal information
    - Incorporating additional sources of age information as they become available, such those shared from a device or app store.

Providers are encouraged to share the findings and outcomes of their reviews and evaluations with eSafety. This includes documenting any changes made in response to lessons learned during early implementation. eSafety will take these insights into account as part of its independent evaluation.

Together, these efforts ensure that regulatory and industry responses remain evidence-based, future-focused, and proportionate to the evolving digital landscape.

2.4 Reasonable steps to prevent age-restricted users having an account

2.4.1 Measures to detect and deactivate accounts belonging to age-restricted users

The SMMA obligation applies to the holding of accounts, including those that existed before the obligation took effect.[78] Providers will need to take reasonable steps to detect accounts that belong to end-users under the age of 16 and be prepared to deactivate or remove those accounts from 10 December 2025.

Providers should also take proactive steps to detect accounts held by age-restricted users on an ongoing basis.

Measures that providers should take to detect and deactivate or remove accounts of age-restricted users include:

- **Using existing end-user data and signals** including location-based signals to infer end-users that are ordinarily residents of Australia, and age-based signals to infer the end-user age or prompt further age assurance processes
- **Providing accessible pathways for people to report potential underage account holders** to trigger further age assurance processes and taking reasonable steps to address vexatious reporting
- **Deactivating or removing age-assured or self-declared under 16 accounts** with kindness, care and clear communication, and taking reasonable steps to prevent account holders who have previously self-declared as under 16 from increasing their self-declared age to avoid account deactivation.

Providers should also ensure end-users have access to accessible **review** options, including the option for suspected age-restricted users to demonstrate they are 16 or over (e.g. via

[78] Section 63E(4) of the Act.

age verification, estimation or vouching), or that they are not ordinarily resident in Australia, to retain an account. This should be accompanied by clear and timely **communications** about what is happening, why it is happening, and where end-users can go for support.

eSafety recommends providers take a successive validation or waterfall approach to detecting and deactivating/removing accounts, starting with measures that are generally less complex, require the provision of less data, and less disruptive to end-user experience.

Use of existing data and signals

The use of existing data and signals with appropriate controls can offer a more frictionless way to infer whether an end-user is ordinarily a resident of Australia and to detect potential age-restricted users, without the end-user needing to provide more information. As highlighted in eSafety's *Behind the Screen* report, age inference is already common practice for many social media services.[79]

Existing data may be sufficient to satisfy providers that the account holder is over the age of 16 without requiring them to submit additional personal information. A reasonably strong indicator could be how much time has passed since the account was created. For example, if the account has been held by an end-user for 16 years, the provider may be reasonably confident that the account holder is over the age of 16. Below are some examples of location and age-related signals that may be used:

[79] eSafety Commissioner (2025), *Behind the screen: The reality of age assurance and social media access for young Australians – Transparency report*, eSafety Commissioner, p. 20.

Location-related signals:

- IP address indicating the person is ordinarily resident in Australia
- GPS or other location services indicating the person is ordinarily resident in Australia
- Device language and time settings indicating the person is ordinarily resident in Australia
- Device identifier indicating the person is ordinarily resident in Australia
- Phone number indicating the person is ordinarily resident in Australia
- App store/operating system/account settings indicating the person is ordinarily resident in Australia
- Photos/tags/connections/engagement/activity indicating the person is ordinarily resident in Australia.

Age-related signals:

- Age of account (e.g. the account has existed for 10 or more years)
- Engagement with content targeted at children or early teens
- Linguistic analysis/language processing indicating the end-user is likely a child
- Analysis of end-user-provided information/posts (e.g. analysis of text indicating age)
- Visual content analysis (e.g. facial age analysis performed on photos and videos uploaded to the platform)
- Audio analysis (e.g. age estimation based on voice)
- Activity patterns consistent with school schedules
- Connections with other end-users who appear to be under 16
- Membership in youth-focused groups, forums, or communities.

Signals may be generated on the platform or they may be received from elsewhere, such as an app store, operating system or third-party vendor.

In most cases, **individual signals should not be relied upon in isolation**. eSafety recommends providers draw on multiple signals – such as profile information, behavioural patterns, and engagement data – to form a more reliable basis for determining that an account is held by end-user who is ordinarily resident in Australia, or that it may be held by an age-restricted user.[80]

[80] In consultations, Stakeholders said they encourage the use of approaches that combine multiple signals; eSafety Commissioner (2025), *eSafety's consultation on the social media age restrictions* [PDF, 331.15 KB], eSafety website, p. 9. The age assurance technology trial report identified good practice for inference models where they discouraged inference based on single variables unless that signal was high-certainty and legally backed (E.7.18). The trial also acknowledged that this needs to be balanced against privacy considerations, referencing best practice in ISO/IEC FDIS 27566-1 which discourages persistent collection or reuse of personal data that leads to the expansion of a user's digital footprint. (E.21.5); ACCS (2025), *Age Assurance Technology Trial – Report*.

For example, where providers seek to rely on IP addresses, eSafety expects providers to detect the use of VPNs, consider **additional signals** that may indicate an end-user is ordinarily a resident in Australia, and then consider the appropriate age assurance measures.

Where platforms rely on bundled signals for the purposes of the SMMA, those signals must be interpreted consistently and in context. This ensures that legitimate changes in how end-users use the platform – for example, a parent engaging with children's content for their child, does not result in loss of account access.

Platforms should leverage existing end-user data and signals to identify and respond to attempts by end-users to bypass age restrictions under the SMMA – including through falsifying age declarations or altering location settings. Providers should **continue to monitor signals over time**; in case there is a change indicating that further age assurance may need to be conducted.

Case study: Good practice

ChatterTrail is a fictitious age-restricted social media platform. Using data shared by end-users through the normal course of their platform engagement and information inferred from that engagement, ChatterTrail's AI generates age inferences based on behavioural and interaction patterns.

For example, after the obligations come into effect, ChatterTrail considers an account that has a self-declared age of 30. This account has been held and in use for 10 years, and the end-user had previously used a credit card to access a premium feature on the service. The platform no longer has the credit card information. However, based on these signals and in the absence of any signals suggesting the end-user is likely an age-restricted user, ChatterTrail considers the end-user is likely not an age restricted user.

In another example, one account was flagged after the end-user frequently commented 'happy 13th,' logged in only after school hours, followed teen-focused pages, and had a network of friends previously flagged as underage. The end-user was informed their account had been flagged, including why and how this happened, and was invited to demonstrate they were aged 16 or over through their choice of facial age estimation or ID-based verification. Following an age estimation result indicating the end-user was likely under 16, the account was deactivated, and the user was provided with information about how to seek a review of the result, when and how they could re-activate the account, how they could access and download their account data, and where they could go for support.

ChatterTrail clearly explains to the end-user the signals and age assurance processes used and provides clear information about how these are applied.

It is eSafety's expectation that providers will be able to provide information on the operation and effectiveness of any tools, technologies and measures used to obtain signals from end-users and provide this information to eSafety when required. Providers should capture and be prepared to report to eSafety the median time it takes to detect underage end-users and the factors that affect this time. See Part 3.1.2 for guidance on what information may be required.

User reporting

Providers should have accessible, intuitive and easy pathways for people to report suspected age-restricted users.

eSafety expects user reporting mechanisms will be clearly identified in plain language and be accessible with a minimal number of steps or clicks from the account or content belonging to the account that, which they wish to report.

Where possible, reporting tools should be available 'in service', meaning an end-user can report the account without needing to navigate to a separate part of the service or exit the service to report via email or complaint form. User reporting forms should be available to all end-users of a service, regardless of whether they have an account or are logged in or not.

End-users should be provided with confirmation that their report or complaint has been received, and an indication of when they will receive a response from the provider. Where appropriate, providers are also expected to provide feedback on the action taken for reports. It may not be reasonable to provide feedback in relation to every report – for example, where doing so would result in the disclosure of personal information, or where the report was vexatious or without merit.

To **prevent misuse of the reporting system**, providers should implement both automated and human review processes to filter out malicious or spam reports. This can help ensure legitimate reports are addressed efficiently while safeguarding users from abuse.

Platforms should ensure all outcomes of user reports are communicated to the impacted end-user, and that appropriate mechanisms to seek review are in place.

eSafety expects providers to be able to provide information to eSafety on the operation of any reporting systems. Providers should track the number of reports received, substantiated, and actioned, and how long this took, and be prepared to provide this information to eSafety.

Deactivating or removing age-assured or self-declared under 16 accounts

From 10 December 2025, **providers should proactively deactivate or remove accounts held by Australian end-users who have self-declared as being under 16**, or those who have returned a result of **under 16 through the platform's age assurance** systems and processes.

eSafety expects that providers have been taking reasonable steps to prevent existing Australian account holders under 16 from increasing their declared age to over 16, opening new accounts indicating they are over 16, or seeking to change their location or other settings in an effort to open or retain an active account on an age-restricted social media platform. Accounts with this type of activity in the lead-up to 10 December should be flagged for review and age assurance.

Providers should keep records of these efforts and be prepared to provide information to eSafety, including information on **how many accounts were deactivated or removed, how many were created, and how many had age or location settings changed**.

Deactivating or removing accounts with kindness, care and clear communication

Providers should approach account deactivation and removal with empathy, sensitivity and the best interests of children in mind.[81]

Prior to any action being taken on an end-user's account, end-users should receive **clear warnings and supportive messaging**. Providers should raise awareness before the SMMA obligation takes effect.

Providers should have regard to **content, functions or features that end-users may have purchased** access to, ensuring the way accounts are deactivated is fair to these end-users.

End-users should be given the opportunity to **download their account information** in a simple, seamless way prior to deactivation or request access to their information from the provider within a reasonable period after account deactivation. The information should be provided in a format that is easily accessible. Providers should consider formats that could allow end-users to transfer their information and content to other services, or to upload the information on the same service if they were to sign up after turning 16. Where reasonable, provider should consult with end-users, particularly those under 16 to understand their preferences and give them options regarding their account.[82]

---

[81] eSafety Commissioner (2025), *eSafety's consultation on the social media age restrictions* [PDF, 331.15 KB], eSafety website, p. 3 and 20.

[82] Where users are close to the age threshold at the time the obligations come into effect, allowing accounts to be reinstated after they reach the age threshold may be beneficial in maintaining connection.

Where accounts have been deactivated, providers must comply with relevant obligations under the Privacy Act in handling the data of deactivated accounts. Providers should not use data or information in deactivated accounts for purposes where end-users have not or cannot provide consent – for example, to train models for AI features on the platform.[83]

Accounts held by age-restricted users **should not be automatically ported** to purported separate services, even if those services are not assessed as being age-restricted social media platforms. Providers may make information about those purported separate services available to end-users, but end-users must provide explicit consent and choose to sign up for the separate service.

Resources tailored for children and young people should be provided using **child-friendly** language, with consideration for culturally and linguistically diverse end-users and end-users with disability. Resources and communications should also be developed for parents and carers, educators and other trusted adults.

Providers are encouraged to co-design their resources with community groups and seek feedback from those groups about their effectiveness and how they can be improved. To promote consistency in messaging, providers are encouraged to **use or amplify the information and resources provided on eSafety's website**.

Wellbeing support pathways – which may include links to support organisations or eSafety's counselling and support services webpage – should be embedded into end-user flows, and staff should be trained in trauma-informed and empathetic communication.

Providers should consider implementing a designated in-app **support channel** to handle reviews and queries related to deactivation.

Providers should also be prepared to provide eSafety with information about their approach to account deactivation, including their communications and wellbeing support pathways, and any feedback or insights gathered.

2.4.2 Measures to prevent age-restricted users from creating accounts

Measures that rely on age-restricted users having an account for an extended period of time before detection would not be reasonable, as this is inconsistent with the objects of the SMMA.

[83] OAIC (2024), *Guidance on privacy and developing and training generative AI models*, OAIC website.

Self-declaration is currently adopted by a number of platforms as the primary method of preventing age-restricted users creating an account.[84] However, even when considered alongside measures to detect and remove account holders, **eSafety does not consider this will be sufficient to meet the obligation**. This is because age inference models generally require an end-user to engage with a platform for an extended period before being detected and removed. Further, solely relying on age inference models to detect age-restricted users may lead to providers collecting more end-user data than would be reasonable.

Reasonable steps a platform can take to prevent age-restricted users from creating accounts include:

- **Age assurance measures** at the point of account creation
- **Measures to prevent age-restricted users from re-attempting account creation** where they have previously attempted to create an account or previously held an account
- **Other general measures to reduce the risk that age-restricted users will attempt to create an account** such as the way a platform is marketed or appropriately listing or publicising the minimum age.

Certain measures at account creation, when used in isolation, will not be fully effective at preventing an age-restricted user from creating an account. Such measures may still form part of a provider taking reasonable steps when considered with other measures at account creation, and other steps taken to detect and remove age restricted users.

Age assurance at the point of account creation

Age assurance at account creation should aim to ensure age-restricted users are not accessing the services and experiencing harm before systems pick them up through age inferences and other detections.

eSafety recognises that implementing age assurance at the point of account creation may change the experience of end-users over the age of 16. The reasonableness of the age assurance measures in place at account creation will be considered having regard to whether the measures would disproportionately impact other end-users from legitimately accessing the service, balanced against the risk to an age-restricted user should they obtain an account.

---

[84] eSafety Commissioner (2025), *Behind the screen: The reality of age assurance and social media access for young Australians – Transparency report*, eSafety Commissioner, p. 43.

eSafety expects end-users will have a choice as to the methods of age assurance they undertake, including at each stage of a successive validation.

Successive validation, or a waterfall approach that escalates only when prior methods are insufficient in isolation or inconclusive – or where the measures create cumulative confidence – is a way to balance assurance strength with end-user experience and proportionate impacts on privacy.

Some age assurance measures that can be put in place at the point of account creation have less impact on end-user experience and can reduce the risk that age-restricted users will create an account. For example, providers should consider whether the use of **cross-platform authentication and interoperable solutions** can be adopted as part of any age assurance process. Examples may include:

- Age signals being shared from upstream services (including app distribution services and devices)
- Sharing age-checks with consent across services operated by the same company
- Allowing end-users to choose to provide a reusable age-assurance result.

Where an end-user creates an account, and the age assurance measures at the point of account creation produce a lower-confidence outcome, providers should adopt additional safeguards until subsequent age assurance is undertaken, or the platform is satisfied that the end-user is over 16. Examples of safeguards may include restricting access to high-risk features and functions and restricting access to certain content.

Case study: Successive validation at account creation to create cumulative confidence

StarClip is a fictitious age-restricted social media platform. When the SMMA obligation takes effect, StarClip uses successive validation at account creation to identify if prospective end-users are age-restricted users.

For example, when a 17-year-old wants to create a StarClip account, StarClip uses geolocation data to determine they are in Australia. The 17-year-old will then be asked to input and verify their email address and self-declare their age, with the prospective end-user listing as 17. StarClip ties this age to the email address to stop prospective end-users from trying several ages.

StarClip also seeks data via an API[85] from an app store or device, which suggests the end-user is above 16, as provided by a parent. StarClip then offers the prospective end-user a

[85] An application programming interface (API) is a set of rules, protocols, and tools that allows different software applications to communicate with each other; Digital Transformation Agency (n.d.), *Application programming interfaces (APIs) – Definition*, Digital Transformation Agency website.

choice between facial-age estimation, voice-age estimation or trusted vouching to confirm their age. The 17-year-old opts for facial-age estimation, and that method tells StarClip they are between 15 and 18. Based on the information StarClip has obtained from the successive validation process so far, they are reasonably confident the end-user is 17 and it would be reasonable to allow them to create the account.

However, StarClip also acknowledges the limitations of the age assurance measures it has used, so defaults the 17-year-old into a safer experience on the platform until they have further age information from signals or the end-user opts to undertake age verification.

Preventing age-restricted users from re-attempting account creation

Where an account is deactivated or removed on the basis that the end-user is under the age of 16, or where an end-user is prevented from creating an account, providers should take steps to prevent children under 16 from attempting to create a new account. Examples of measures platforms can take include:

- Collecting non-identifiable identifiers from end-users on registration or sign up before undertaking age assurance, to assist in flagging re-entry attempts. This could include non-identifiable account metadata, IP ranges, pattern recognition, device identifiers or other identifiers
- Requiring end-users to authenticate their accounts on sign-up by sending an authentication code or message or link to an email address or phone number used to create an account (including multi-factor authentication). This means that an account must be linked to a valid email or phone number. Creation of a new account can be blocked where that email or phone number was associated with an account that has just been deactivated, removed or refused
- Implementing a device block to prevent an account from immediately re-registering on the same device.

Other measures to prevent age-restricted users creating an account

Reasonable steps to prevent an age-restricted user from having an account include the conduct of a platform in engaging with age-restricted users.

Providers should take **proactive steps to reduce the risk that age-restricted users will attempt to create an account** including:

- Using positive behavioural cues and prompts to redirect or dissuade age-restricted users from creating an account
- Ensuring marketing of the platform is directed towards end-users over the age of 16

- Listing the services as 16+ for Australia on app distribution services
- Appropriately reflecting age restrictions in terms of use, end-user communications and policies
- Reducing the discoverability of the service to age-restricted users.

Platforms should not incentivise age-restricted users to access the platform and create an account.

2.4.3 Measures to prevent, detect and respond to circumvention

Preventing circumvention is a key factor for providers in meeting the SMMA obligation.[86]

Circumvention methods that age-restricted users may attempt to use include methods of **identity- or age-based circumvention** or **location-based circumvention** such as the use of VPNs; relying on other age verified end-users; creation of false **identity documents;** the use of AI or deepfakes to spoof age estimation systems; clearing cache or browser history to reset age checks; answering knowledge-based questions with guessed or known information; and the use of hand-me-down devices that retain age assured end-user credentials.

Providers must take reasonable steps to respond to the methods of circumvention that are **easily accessible to age-restricted users** or to methods that it is **reasonable to assume an age-restricted user may seek to use**.

Examples of steps providers may take to prevent, detect and respond to circumvention

- Preventing changes to self-declared age unless age assurance is undertaken
- Ensuring age assurance measures incorporate liveness checks
- Preventing and monitoring changes in account details that may indicate improper transfer of account ownership (e.g. the sale of an account to an end-user under 16)
- Monitoring for multiple accounts from the same device or IP address
- Using device telemetry, behavioural signals, and other persistent identifiers to detect irregular activity
- Integrating VPN detection services and IP intelligence APIs to flag and restrict high-risk IP ranges

[86] eSafety Commissioner (2025), *eSafety's consultation on the social media age restrictions* [PDF, 331.15 KB], eSafety website, p.5.

- Using geolocation consistency checks to identify mismatches between IP address and declared location
- Implementing systems to detect and investigate suspicious IP switching
- Considering additional signals that can indicate likely location.

Where providers detect irregular behaviour or suspect circumvention, they should consider whether that end-user is ordinarily resident in Australia and an age-restricted user, and whether further age assurance is required.

Where a provider identifies that an individual end-user has circumvented or bypassed age assurance technologies, the provider should take reasonable steps to reduce the risk that other end-users will circumvent in the same manner.

Without limiting the expectation that providers will provide transparent and accessible information on age assurance measures, providers should ensure any information they publish does not facilitate or enable age-restricted users to circumvent the measures.

2.4.4 Allowing end-users to make complaints or seek review

Providers should offer accessible, fair, and timely complaints or review mechanisms for end-users in relation to:

- Any adverse outcomes resulting from any **age assurance processes**
- Any adverse outcomes resulting from **reports** of underage accounts
- account **deactivation/removal decisions**.

Providers should clearly communicate how and when end-users can make a complaint or seek review of a decision they believe was made in error. Providers are also encouraged to make it clear to end-users that they can make privacy complaints to the OAIC.

These mechanisms should be **accessible and inclusive**, allowing end-users to navigate the process **with clarity and relative ease**. These mechanisms should be clear and readily identifiable to end-users at the point a decision is made about their account. For example, if an end-user receives a notification or an email with an outcome or decision relating to their age and access to an account, they should be provided with information about how to make a complaint to the provider or seek review in that communication.

When requesting additional information as part of this process – such as identification – **providers must not require end-users to provide government-issued identification material without also providing a reasonable alternative means for end-users** to assure the provider

that they are not an age-restricted user.[87] The same considerations set out in this guidance apply here regarding reasonable alternative measures to assess age.

End-users should be notified when their complaint or application for review is received, along with an expected timeframe for a response. They should also be informed of how their complaint, dispute or request for review was assessed – whether by a human moderator or an AI system.

In alignment with best practice approaches to artificial intelligence and automated decision-making, there should be human in the loop or human oversight to mitigate the risks of incorrect decisions – including unreasonably blocking or removing accounts that don't belong to age-restricted users.[88] **Fully automated reviews should be avoided**.

Providers should also equip end-users with a mechanism to provide feedback to the service in relation to the effectiveness of age assurance measures, and a point of escalation where end-users can communicate any issues they have experienced with age assurance technologies and surrounding systems and processes.

Providers should ensure they are monitoring and recording relevant metrics and indicators of end-users' experiences in making complaints disputes or requesting review. For example, if a high number of successful complaints or reviews are being made about a particular tool or technology, this can be a useful indicator of the effectiveness and performance of that tool or technology.

By way of further example, if a significant number of complaints or reviews are made by end-users about one tool, technology or process – but not others – this can be an indicator that end-users are not able to find or use the mechanism to make complaints, disputes or request review for those other tools, technologies or processes.

Providers are well placed to determine what metrics should be monitored and tracked in relation to complaints, disputes and reviews, and should ensure they are able to report to eSafety when required to do so.

2.4.5 Policies, people, processes and record keeping

Terms of use, standards of conduct, policies and procedures

Terms of use, standards of conduct, policies and procedures are key mechanisms for providers to communicate what is and is not allowed on their platform and the minimum

[87] Section 63DB(2) of the Act.
[88] See generally: eSafety Commissioner (2025), *Safety by Design Overview* [PDF, 696 KB], eSafety website, p. 36; Department of Industry, Science and Resources (n.d.), Voluntary AI Safety Standard - *The 10 guardrails*, Department Industry, Science and Resources website.

age for end-users of their service. **Providers should ensure that terms of use, standards of conduct, policies and procedures** for the service**,** and information available to end-users include:

- a clear statement on the minimum age requirements for having an account
- the age assurance processes in use on the platform
- the data collection, use and retention policy
- the review processes
- the reporting processes
- the account deactivation processes, and how to save and export data for those accounts.

Terms of use and policies should advise against vexatious reporting and providers should specify and enforce consequences for those who misuse reporting channels.

Trust and safety resourcing and oversight

Providers should ensure trust and safety functions are adequately resourced to support the implementation of measures to meet the obligation, including:

- evaluating impact and effectiveness of age assurance measures across the end-user experience,
- reviewing and responding to reports of potential accounts held by under 16s, and
- managing requests for review of decisions and outcomes.

eSafety expects trust and safety functions and implementation of measures are subject to an **adequate level of oversight and accountability** by senior management including through regular reporting.

Where trust and safety functions are contracted out to external third-party vendors, the provider remains responsible for any outsourced functions and having appropriate oversight in place. In eSafety's view, it is optimal for providers to integrate their trust and safety function into the culture of their business.

Platforms may experience an increase in end-user reporting as a result of the SMMA obligation, and eSafety expects providers to take reasonable steps to **ensure their systems can respond to increased reporting and provide a timely and fair outcome**.

The SMMA obligation is not a complaints scheme directing reports to the regulator, therefore, eSafety expects providers will accept and manage all end-user reporting and disputes.[89]

Information about trust and safety resourcing and oversight for purposes of complying with the SMMA obligation should be recorded and providers should be prepared to provide this information to eSafety.

Training

Providers should ensure relevant staff receive effective training to understand the provider's obligations and to ensure the performance of their duties is consistent with this guidance.

While not exhaustive, relevant staff may include trust and safety teams, legal, privacy and compliance teams, product designers and developers, engineers, as well as marketing, communications and community engagement teams.

Training should not be limited to providing this guidance. Providers should ensure staff are aware of the platform's internal policies and procedures relevant to preventing age-restricted users having accounts. Staff should be provided with training to support them to enforce these policies in a manner consistent with the guiding principles set out in this Regulatory Guidance.

Providers should ensure training is undertaken periodically, recorded, and updated regularly to support continuous improvement and responsiveness to emerging risks and changes in the platform.

Investing in systems, tools and processes

Providers should invest in appropriate systems, tools and processes to implement reasonable steps to comply with the SMMA obligation and to support continuous improvement in the detection and prevention of age-restricted users on the platform. This should include testing and improvement of existing tools, as well as innovation of new tools such as advanced AI tools to improve compliance with SMMA and enhanced safety by design.

Investment is **not limited to financial investment** and could also include initiatives such as participation in and support for research, pilot projects, and collaboration with non-government and government organisations or cross industry collaboration.

---

[89] Complaints about an interference of privacy of an individual as defined in subsection 63F(1) and (3) of the Act can be considered by the OAIC. Providers should make users aware of this pathway as relevant.

This investment should be tracked and providers should be in a position to give this information to eSafety.

Record keeping

Providers should implement effective record keeping practices to provide transparent information that explains the measures they implement to comply with the SMMA obligation and monitor the effectiveness of those measures. This is important to **ensure providers can demonstrate how they are taking reasonable steps in the context and circumstances of the platform and its end-users**.

Providers should retain an appropriate amount of detail to assist eSafety to assess the effectiveness of the measures, whilst ensuring compliance with relevant privacy legislation. **Information about individual end-users, their unique age assurance checks or outcomes is not necessary to demonstrate the taking of reasonable steps**. Rather, providers should be prepared to report on the systems, processes, tools and technologies they implement to comply with the SMMA obligation.

See Part 3.1.2 for more information on the types of information and data that eSafety may require to assess compliance with the Act.

Part 3: eSafety's approach to compliance monitoring and enforcement

eSafety's focus is on ensuring those platforms who meet the threshold as an age-restricted social media platform comply with their SMMA obligations. eSafety takes a strategic and where appropriate, graduated approach, to compliance and enforcement as set out in eSafety's Compliance and Enforcement Policy.

Whether a provider has taken reasonable steps will include an assessment of the holistic impact of all steps taken by a provider, across the service. Measures will not be evaluated in isolation. This is about **systems and processes**, not individual accounts.

The presence of accounts belonging to age-restricted users on a service will not necessarily be taken to mean that a provider is non-compliant if the provider can otherwise demonstrate it took reasonable steps to prevent age-restricted users from having accounts.[90]

eSafety will take a proportionate and risk-based approach to monitoring providers' compliance with the SMMA, initially focusing on ensuring compliance by providers with the greatest numbers of Australian children under the age of 16 prior to 10 December, and those platforms that utilise the persuasive design features associated with the risk of harms to children.

Acknowledging that providers vary significantly in their technical sophistication, resources, and maturity, eSafety will consider the technical and commercial feasibility of measures adopted by providers.

eSafety will also consider the ecosystem and market – including what tools and technologies are available to providers, and the associated cost. This is not a static consideration and will change over time.

eSafety expects **all providers** to focus on the **detection** and **deactivation/removal of existing accounts** held by children under 16 and prevent those users from immediately creating a new account.

[90] *'It is not the intention that the Bill would punish a platform for individual instances where young people circumvent any reasonably appropriate measures put in place by the platform – however, a systemic failure to take action to limit such circumventions could give rise to a breach.'*
EM, *Online Safety Amendment (Social Media Minimum Age) Bill* 2024 (Cth), p. 2.

eSafety encourages providers to engage proactively with eSafety to support their compliance with the SMMA obligation. This can include proactively notifying eSafety of challenges in implementation, newly identified gaps in processes or unforeseen consequences and impacts of implementation.

3.1 Compliance activities

eSafety will consider a range of compliance and enforcement options under the Act, and where appropriate, work with providers under a voluntary arrangement to ensure compliance.

As noted above, eSafety will be taking a proportionate and risk-based approach to compliance, initially focusing on **services with the greatest number of end-users**, where there are **higher risks of harm**, accounting for the steps providers are implementing to prevent the **youngest users** from having accounts.

Consistent with this approach, eSafety will also monitor for migration of age-restricted users and remain agile in its compliance approach, including enforcing compliance through other regulatory powers under the Act.

eSafety will consider a number of factors when assessing whether a provider of a service has complied with the SMMA obligation, including but not limited to:

- the risks related to the service, including:
    - number of Australian account holders
    - the risk and evidence of online harms
    - design features and functions related to harms
- the effectiveness and proportionality of the steps taken by a provider in meeting the SMMA obligation
- technical or practical limitations to implementing certain steps
- substantiated information establishing that a provider has plans to take further action or other steps in the short to medium term.

3.1.1 Deactivation and removal of accounts

Having engaged and consulted with various stakeholders including children and young people, eSafety recognises that there is a strong preference for existing end-users that are under the age of 16 to be given the choice of having their accounts removed or deactivated/suspended (with their data retained by the provider) until they reach the age

of 16. This was particularly the case for children who are almost 16 years of age where having the option to reactivate their account and keep their connections once they reach the age of 16 was expressed as the preferable outcome.

For this reason, eSafety's focus in monitoring compliance and enforcement will be on the steps taken by providers to prevent age-restricted users from having **active** accounts. Providers must ensure they comply with their privacy obligations in respect of deactivated or suspended accounts.

Memorialised accounts

eSafety understands that some providers enable accounts to be 'memorialised' in honour of the account holder who has since passed away, and that by virtue of this memorialisation, the account is converted into a page which is only accessible in a viewable format and therefore cannot be accessed in a logged-in state. Accordingly, eSafety takes the view that accounts that have been memorialised are not captured by the SMMA obligation because the age of the individual to whom the memorialised account previously belonged is not relevant, as no one 'has' the account.

Additionally, eSafety considers that accounts that are in the name of an age-restricted user who is deceased but have been subsequently taken over by another end-user (for example, by accessing log-in credentials or by way of 'legacy contact') should be assessed as being held by that new end-user. For example, where a parent takes over the account of their deceased child who was an age-restricted user at the time of passing, that parent is now the account holder of that account.

3.1.2 Information-gathering powers

eSafety has information-gathering powers under s 63G of the Act. Section 63G(1) enables the Commissioner to obtain **any information** from a provider that is relevant to their compliance with the SMMA obligation and compliance with sections 63DA and 63DB (see Part 1: Legal, regulatory and technological context above for further information).

Section 63G(3) of the Act also enables eSafety to obtain any information from a provider of an electronic service that is relevant to whether the service is excluded or included as an age-restricted social media platform under the legislative rules.

The recipient of a s 63G notice must comply with the notice to the extent that they are capable of doing so.[91] Non-compliance with a s 63G notice may be subject to enforcement action including civil penalties of up to $825,000 for each contravention.[92]

eSafety will use the information-gathering powers in s 63G to obtain information about a provider's systems and processes in relation to the providers' age assurance measures to detect Australian children under 16 and prevent them from having accounts on their service. This may include, and is not limited to, specific and granular information and data about:

- Whether any tools or technologies are used to assess the age of prospective or existing account holders, including the names of all tools/technologies and what technical indicators each tool/technology used
- What steps providers took when a tool, technology or indicator assessed that they were of an age that required action (for example, under the permitted age of 16)
- Whether providers undertook research to develop or implement new or additional tools to assess the age of account holders
- What mechanisms were in place to enable end-users and others to make reports of potential underage account holders (including how many steps were required to start and complete a report)
- The number of account deactivations/removals due to an account holder being under the permitted age of use, and the proportion of these made as a result of proactive detection (use of tools and technologies) and as a result of third-party reporting
- Steps taken to prevent end-users whose accounts have been deactivated/removed from immediately re-registering an account with the service, including use of technical and other indicators
- The number of new accounts created in Australia after 10 December when the SMMA obligation comes into effect
- Relevant internal and external-facing documents.

Providers should document and evaluate their efforts to prevent and detect circumvention and be prepared to provide eSafety with information about their effectiveness, as well as any observations or insights to inform eSafety's enforcement of the SMMA obligation and broader ability to promote children's online safety.

---

[91] Section 63H of the Act.

[92] Section 162 of the Act. The penalty is 500 penalty units (section 63H of the Act). Under section 82(5)(a) of the Regulatory Powers (Standard Provisions) Act 2014 (Cth), the maximum penalty for a body corporate is 5 times the pecuniary penalty (in this case, 500 penalty units). As of September 2025, one penalty unit amounts to $330 as set out in section 4AA of the Crimes Act 1914 (Cth).

eSafety will also use its information-gathering powers to obtain information regarding the effectiveness of the steps taken by providers, which will likely include requiring providers to provide data on the number of account holders of various ages both prior to and after 10 December 2025. Other relevant metrics and questions which may be required include:

- Whether tools or technologies were used on all relevant parts of a service (for example, whether language-analysis technology was used on public posts as well as direct messages and profile bios etc.) and at what point tools or technologies were deployed (for example, at point of account creation, proactively once an end-user had created an account or at any other point)
- Whether providers had undertaken an assessment of the accuracy of each tool/technology, and the results of the assessment/s
- Information about end-user and other third-party reports, including median time to reach an outcome after receiving a report, the proportion of reports that were reviewed by a human moderator/staff of the service and actioned, and number of reports made that were not reviewed and not actioned
- The number and nature of successful challenges and accompanying information provided to end-users
- Which indicators were responsible for the majority of account deactivations.

This is a **non-exhaustive list**. Providers should ensure they have processes in place to be able to demonstrate compliance with the SMMA obligation to eSafety when required to do so.

3.2 Platform provider notifications

If eSafety is satisfied that a provider has contravened the SMMA obligation by any one of the following:

- failing to take reasonable steps to prevent Australian children under 16-year-olds having accounts
- collecting information that must not be collected[93]
- not providing a reasonable alternative means to collecting government-issued identification, or using an accredited service under the Digital ID Act to comply the SMMA obligation[94]

[93] As at the time of this guidance, no legislative rules had been made specifying a kind of information that must not be collected as provided for under section 63DA(1) of the Act.
[94] Section 63DB(1) of the Act.

then eSafety may prepare a statement to that effect, give a copy of the statement to the provider and publish the statement on the eSafety website.

3.3 Enforcement

eSafety may take enforcement action where a civil penalty provision of the Act has been contravened including when enforceable notices are not complied with. The enforcement action may include:

- giving an infringement notice[95]
- accepting an enforceable undertaking[96]
- seeking court-ordered injunctions[97]
- seeking court-ordered civil penalties.[98]

Non-compliance with the SMMA obligation has a maximum penalty of 30,000 penalty units. For civil penalties against a body corporate (including an online service provider) the maximum penalty is 150,000 penalty units, currently the equivalent to $49.5 million.[99]

[95] Section 163 of the Act.
[96] Section 164 of the Act.
[97] Section 165 of the Act.
[98] Section 162 of the Act.
[99] This is due to the application of section 82(5)(a) of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) which specifies that the maximum penalty for a body corporate is 5 times the pecuniary penalty (in this case, 30,000 penalty units). As of September 2025, one penalty unit amounts to $330 as set out in section 4AA of the *Crimes Act 1914* (Cth).

Appendix A: Key terms

In this document, **'age assurance methods'** is used to refer to the underlying approach used to determine age – for example, verifying a date of birth from an ID or facial age analysis. **'Age assurance systems'** is used to refer to both the method and how it is implemented –including, for example: whether it uses secure ways to store or transmit data, or the specific practices and configurations set in relation to buffer thresholds.

Throughout this document **'measures'** is used to refer to the steps a provider is taking to comply with the SMMA obligation. This could include implementing age assurance, or other practices including making end-user reporting available or taking action to detect circumvention attempts.

Age assurance result means information produced by an age assurance system indicating that an individual is a certain age, over or under a certain age or within an age range.

Age-based eligibility decision means action by a relying party to determine access to goods, content, services, venues or spaces based on an age limit or an age band.

Age-restricted user means an Australian child who has not yet reached 16 years of age.

Age-restricted social media platform has the meaning in s 63C of the Act.

Australian child means a child who is ordinarily resident in Australia.

Buffer threshold means a configurable margin around the age restriction that accounts for the inherent uncertainty in age estimation.[100]

End-user means a person that directly interacts with an online service or application for its intended purpose.

End-users in Australia are users of an online service who are physically located in Australia.

Identity document means a physical or digital document issued by an authoritative party containing identifying attributes.

Material includes content in the form of text, data, speech, music or other sounds, visual images (moving or otherwise) or in any other form, or combination of forms.[101]

Messaging may be enabled through a range of features and functions such as direct/private message (whether one-to-one or involving multiple end-users) and chat functions.

---

[100] ACCS (2025), *Age Assurance Technology Trial – Report*, D.9.3.
[101] Section 5 of the Act.

Online social interaction broadly encompasses an end-user's engagement with other end-users or their material through an electronic service, whether active or passive, including by communicating, sharing material,[102] participating in communities and expressing reactions.

Post material means material 'posted' by end-users if it is accessible to, or delivered to, one or more end-users on the service.[103] This includes material posted in a direct message or group, as well as on an 'open' or public space such as a profile, feed or page.

Purpose, as it appears in the Act, means the objective for which anything exists or is done, made, used etc.[104]

> **Significant purpose** is a purpose which is important and meaningful rather than one which is merely incidental or subsidiary.
>
> **Sole purpose** means the only purpose.

Technology stack means the collection of the infrastructure and services enabling the use of a website or app. **Technology stack deployment** refers to the strategic placement of age assurance mechanisms at different layers of the digital infrastructure – ranging from end-user devices and operating systems, to networks, app stores and backend services.[105]

[102] Section 63C(2) of the Act.
[103] Section 11 of the Act.
[104] *Macquarie Dictionary Online* (2025).
[105] ACCS (2025), *Age Assurance Technology Trial – Report*, Part J.7.2.