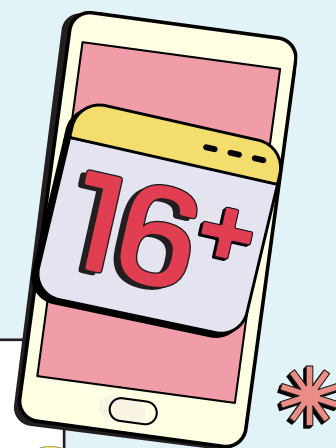


Access to **social media** is changing

The Australian Government has made some new rules about who can create or have an account on social media in Australia.

This is called 'social media minimum age' (SMMA) but sometimes it is also referred to as the social media 'ban', 'delay', 'age requirement, or 'age obligation'.



Creating or having an account on social media will mean that personal information will be looked at

To follow the new rules, social media companies will need information about:

- 1) if you ordinarily live in Australia, and
- 2) if you are over the age of 16.

This information will likely be personal information, which is information that could reasonably identify a person.

There are many ways that social media companies could check if a person usually lives in Australia.

They might look at information like:

- Australian mobile number
- Wi-Fi information
- GPS location information
- app store, operating systems and account settings
- photos, tags, connections and online activity that a person or others have shared on social media.



From **10 December 2025**, social media companies will have a responsibility to make sure everyone using their service in Australia is at least 16 years old. To do this, they will need to handle some personal information.



eSafety have helpful resources that explain what SMMA is, why it was introduced, which social media platforms it affects and how to have conversations with the young people in your lives about this change. Check out www.eSafety.gov.au



The Office of the Australian Information Commissioner (OAIC) is here to protect the privacy of all Australians. We will make sure that social media companies, and any company they team up with to do age checks, called 'third parties' or 'age assurance providers', obey the law and protect your personal information when following these new rules.



There are many ways that social media companies could check a person's age. And they might want to use a few different ways to check. They may even team up with outside companies known as 'third parties' or 'age assurance providers' to be sure they got it right.

Start a conversation!

‘ Access to social media is changing on 10 December. Everyone will need to be over the age of 16 to create or have a social media account. ’

‘ Social media companies will need to check if you are old enough and make sure you live in Australia. To do that they will need to look at information about you. ’

‘ How do you feel about sharing your information with social media companies and companies they team up with, to check your age and location? ’

Age assurance methods

Age inference

Some methods to check a person's age happens in the background. These methods may look at who they follow, how they speak, when they post and when the account was created to suggest what their age is, based on information the person has already shared.

These methods are called **age inference** because they *infer*, which means to suggest based on evidence, what your age is.

Age estimation

Other methods might ask a person to do a task like take a selfie or video to look at physical features like their face or how they move their body or listen to their voice. These methods use artificial intelligence (AI) and statistics to guess what a person's age or age range is.

These methods are called **age estimation** because they *estimate*, which means to guess, your age or age range based on information such as physical features or behaviour.

Age verification

A person might also be asked to share an image of their government-issued ID like a learner's licence or passport to check their date of birth or sign into another online service that knows their age. These methods check a person's age by looking at systems that already know their age.

These methods are called **age verification** because they *verify*, which means to confirm, your age with official information. Social media companies are not allowed to force a person to use government issued ID to prove their age online. They must offer other methods to check a person's age.

Age assurance methods

may look like



Behavioural analysis

Seeing if you behave like a child



Biometric estimation

Taking a selfie or using your voice



Physical gesture

Looking at how you move your body



Hard identifiers

Sharing your official documents



Age tokens

Signing into another online service

Privacy + Tips

Tips on how to have a conversation about online privacy

Children and young people need support online, just as they do offline. Sharing personal information online can be risky, so it's important to educate children and young people on how to make good decisions and limit those risks.

Start the privacy conversation

To help the young people in your lives protect their personal information and their privacy, it is essential that you talk to them about what these terms mean and why they are important.

Personal information is information that could identify a person. Privacy is about protecting personal information.

Privacy is very important to young people's ability to make decisions about how to live their life, what to believe and what to think. Privacy also offers young people personal safety, protection from scams and identity theft.

The key message is that we can protect our privacy by protecting our personal information.

Discuss their digital footprint

Young people need to know that their digital footprint can last forever. Our digital footprint is the information we leave online. Make sure that the young people in your lives know the difference between the kinds of information that may be appropriate to share online and what should be kept private.

Look carefully at what information is required for the age check (such as login details like an email or phone number) and whether there is information that you do not need to provide to access the service (such as address or gender).

Encourage safe and smart device use

Children and young people store a lot of personal information on their phone, tablet and laptops, so it is important they use security measures to protect this information.

Secure all devices with a pin lock, passcode or passphrase. Create multi-factor authentication or 2-Step verification to protect online accounts. Make sure the young people in your lives know that someone could gain unauthorised access to their social media accounts, private message, personal photos and more if they don't secure their device.

Ensure children only download apps from reputable sources, especially if they are sharing location or financial information. It is also important that you know what apps and online services the young people in your life are using and what information they are providing to access the service.

Encourage young people to stop and think

Personal information is valuable like treasure. Encourage young people to hold onto it carefully and don't share it without good reason.

Be on the watch out for scams. Scammers often pretend to be trusted organisations such as the government, banks, or social media companies. Scammers might try to trick young people into signing into their account. Only share personal information with trusted websites. Look for secure websites that start with **https://**

Encourage young people to talk to a trusted adult if something feels off or if they are not sure about what information they are being asked to share.



Start a conversation!

‘ Do you think sharing your personal information when it is not needed, is worth the risk to your privacy? Do you think this is a ‘good’ trade-off? ’



Privacy means being in control of your personal information

Personal information is information that could identify a person like their name, address, email, phone number, school, date of birth and photographs. It also can be things like a person's location and opinions.

Personal information can be protected by not sharing it, when it is not needed.

Young people under the age of 16, have a choice to make:

Trying to have or create a social media account means sharing their personal information when it is not needed

Waiting till they are 16 to have or create a social media account means they will be sharing their personal information for a purpose.

If you think personal information has been mishandled, make a complaint

If you think a social media company or third party has used or shared the personal information of a young person in your life, **make a complaint to the social media company or third party**. If they don't respond to your complaint, you can make a complaint to the OAIC.

A step-by-step guide on how to make a complaint is available on our website: www.oaic.gov.au/privacy/privacy-complaints

If you have any questions about SMMA such as what do to if your account has been mistakenly deactivated, eSafety has resources to support you. Check out www.eSafety.gov.au

