

Legal Yarns

Online safety





What is online safety?

Online safety is about being aware of risks and your responsibilities when you're using the social media and the internet. It includes making sure that your online footprint is safe and secure, checking that you have secure passwords for your accounts and up-to-date software, and protecting yourself against cyber-bullying and online sexual abuse. If you have children, it is important to make sure they are safe online as well.

Why is online safety important?

Online safety is important, because there are so many risks when you use the internet. Whether it's for communicating, shopping online, doing online banking, or for school or work, we use the internet every day, and it holds our personal information and data.

While the internet makes a lot of things easier and quicker, it is important to protect your personal information and data, be aware of the risks, and know your rights and responsibilities.

What is covered in this Legal Yarn?

Learning to be smart online is easy. We can take you through the following key issues to think about when using social media and the internet.

1. Social Media and Young People
2. Privacy
3. Self-Incrimination
4. Cyber-bullying and Harassment
5. Online Sexual Abuse
6. Resources and Support

Our upcoming Legal Yarn on Identity Theft and Scams is also an important resource.





Why is it important to look out for each other online?

Making sure our young ones, Elders and people with disability are safe online

Children and young people are online for both schooling and personal use, so parents, family members, teachers and carers need to help their young ones learn how to use social media and the internet safely. Young people may be particularly vulnerable to cyber-bullying and online sexual abuse. Parents also need to responsibly monitor how much their children are using the internet and what they are using it for.

Other community members, including our Elders and people with disability, may need support with digital literacy. Scammers target vulnerable populations including Elders and people with disability. We can all look out for signs that someone is being scammed, threatened or cyber bullied.

SOCIAL MEDIA AND YOUNG PEOPLE

What's the social media ban for young people?

As of 10 December 2025, children under the age of 16 cannot access certain social media accounts.

The aim of these age restrictions is to reduce the harm that children and young people can be exposed to online and to give young people more time to develop real world connections in other ways.

What social media is banned for under 16 year olds?

The following social media platforms must prevent access to children and young people who are 16 years or younger: Snapchat, TikTok, Facebook, Instagram, X, Kick, Reddit, Threads, Twitch and YouTube.

What social media can people under 16 years old use?

Platforms that are only for messaging like Messenger, WhatsApp and online gaming can still be used if they don't come under this age restriction. YouTube Kids can also be used.





Can I get in trouble if I'm under 16 and I use social media?

No, you and your parents/carers won't get into any trouble if you have an account and are 16 years or under, but the platform could face penalties if they don't undertake steps to prevent use of underage accounts.

You will still be held accountable for how you behave and engage online.

How do I keep my child or young person safe?

It's important that parents and carers actively monitor what and how our young people engage online. There are apps that can support this, but open communication about expectations is important to keep children safe.

You can find out more information about social media restrictions through the [eSafety Commissioner website](#). You can also check out [factsheets about the social media restrictions](#) on eSafety websites. The eSafety Commissioner also has deadly [First Nations resources](#) available on their website.

PRIVACY

How does being online impact my privacy?

It's best to be careful about what you post online because once something is online it can be hard to delete it, or control who shares it.

For example, even if you delete or deactivate your Facebook account, your information does not automatically disappear. Your photos, posts and comments can still be available through archives or old versions of websites, or in the comments you've made on other people's pages.

Even if you delete a post or photo from your social media site, it can still be retrieved. For example, removed and deleted information on Facebook may be stored in backup copies for up to 90 days.

People can also take a snapshot or save posts and photos and reshare these without your permission. If you're not sure, check with a trusted adult.

How can I protect myself against fake profiles and accounts?

It's also important to know what a fake account or profile is. There are people, trolls, AI, companies that use fake accounts, to spread hate, bully and troll people. Fake accounts can also seek to scam you, steal your money and/or





your identity. They might want to add you as a friend on social media. Anyone can make fake accounts, including the police if they suspect criminal activity.

It is important to not accept friend requests from people you don't know. If the police suspect that you or your friends have committed a crime, they can apply to the court to be able to search your social media accounts for evidence.

To learn more about identity theft and scamming, read our Legal Yarn on Identity Theft and Scams.

Can police seize and access my phone, laptop, tablet or hard drive?

Generally, police need a warrant to seize your phone or a digital device. However, there are some exceptions. For example, if they reasonably believe you have committed a serious crime and the phone contains evidence of the offence; or in circumstances where they believe it is necessary to seize the device to prevent the destruction of evidence.

Just because police can seize your device, doesn't mean they are able to access its contents. Accessing data is treated more carefully and usually police need to obtain a warrant to access the data from the confiscated device. There are some exceptions to obtaining a warrant, such as circumstances involving very serious matters relating to terrorism or child exploitation, where you may be required to give the police your code to access your phone.

More commonly, police will try to obtain your permission to look through your device or ask you to unlock the phone. They may do this to avoid having to obtain a warrant. The police may present these requests as co-operative or informal. You do not need to provide your consent for police to access your data in these circumstances, and you should immediately ask to seek legal advice.

If police want to seize your phone or access information from it, you should seek legal advice. Call VALS on 1800 064 865.

Can schools and work see my information?

If you use a school or work computer or phone to access your accounts, you must follow their "acceptable use policy". This policy will usually give your school or employer the right to monitor your computer use. This means they can see the search history and usage when you're using a computer at your school or work.

If there is something you don't want your school or employer to see, don't use their computers or phones to look at it. For example, it might be smart to





avoid logging in to personal emails, bank accounts and social media accounts on your school or work computer or phone.

Schools and workplaces usually can't look at your personal phone. Many schools ban the use of phones during school time.

SELF-INCRIMINATION

What is self-incrimination?

Self-incrimination is when a person says or does something that links them to a crime. For example, any public comments, pictures or videos you post online can be seen by anyone and be used as evidence if you are accused of doing something wrong or unlawful. Even if you use an anonymous username, this may not protect you.

Anyone who is found guilty of committing a serious violent offence (like motor vehicle theft, robbery, aggravated burglary, carjacking, or home invasion) and had posted an image or video of committing the offence can be charged with an additional 'post and boast' charge, and may receive up to an additional two years' imprisonment.

How can I avoid self-incrimination?

How you conduct yourself online is important. Information you post online should be truthful and accurate. Online activities such as cyber-bullying or sexting may have legal consequences. For example, if your online activity incites violence, causes harm or is hateful, you could be held accountable for a crime.

If there are any Intervention Orders in place, you also need to be careful that information you put online in posts or messages does not break court orders such as Intervention Orders. For example, if there is an Intervention Order in place that requires no-communication, contacting the protected person online is treated the same as contacting them in person and can result in penalties, or further charges.

CYBER-BULLYING & HARASSMENT

What is cyber-bullying and harassment?

Cyber-bullying is when someone or a group of people target an individual, or group of people online in a demeaning and harmful way. This can include





harassment on online forums, negatively commenting on social media posts, excluding someone from group chats, tracking someone's location, sending cruel and demeaning messages or posting images and/or tagging someone without their consent. Cyber-bullying can be very harmful to an individual, their families and community.

If you or someone you know has been impacted by cyber-bullying you can access support through the [Kids Helpline](#), [Dolly's Dream](#) and [Lifeline](#).

What happens if I cyber-bully or harass someone?

Cyber-bullying can be a crime. If you, or a group of people you are involved with cyber-bully a person, or a group of people, you can be penalised for doing so. The police may choose to investigate and hold those responsible accountable.

What should I do if I get bullied or harassed online?

Cyber-bullying may be a crime if it involves using the phone or internet in a menacing, harassing or in an offensive way. You can call VALS to seek legal advice if this has happened to you. You can also make a report to the eSafety Commissioner.

eSafety Commissioner

The commissioner can investigate cyberbullying of children, adult cyber abuse, image-based abuse (sharing, or threatening to share, intimate images without the consent of the person shown) and illegal and restricted content.

You can make a report online through the [eSafety Commissioner's website](#).

SEXUAL ABUSE ONLINE

What is sexting?

Sexting is when someone is using messaging platforms to take, ask for, receive, send or share intimate photos or videos including where someone is naked, partly naked, posing sexually or doing a sexual act. Sharing an intimate image or video of someone without their consent is image-based abuse and is a crime.





Is it illegal to share sexual images or videos of others?

Sexting can be a crime if it involves people under 18, even if it is of themselves, or the other person has said it's OK. Images or videos which show someone under 18 in a sexual way are called 'child abuse material'.

Child abuse material can be photos or videos, but also other images like drawings and even cartoons. It also includes pictures that have been photoshopped or digitally altered to make the person look young or naked.

Is it illegal to share sexual images or videos of yourself?

If you are under the age of 18, it is illegal to share sexual images or content of yourself, even if you feel comfortable sharing it with your partner.

This law is in place to protect you against the risks, including that you may have been coerced into doing this, and you cannot control what happens to the images or videos after you share them.

What should I do if I get asked to, or have shared sexual content?

If you were pressured by someone to send intimate photos of yourself, this is a crime. You should let a trusted adult know, report it to police and seek legal advice.

Check out our [Lubly Affirmative Consent Resources](#) on our website for more information about consent.





Where can I get help?

If you have concerns about Online safety and the topics covered in this Legal Yarn or if you would like more information, or to speak to our legal teams, you can **call VALS on 1800 064 865**.

You can find out more information about our legal teams and the types of issues they can help with via [our website](#).

Disclaimer

This document contains general information only and does not constitute legal advice or services.

This fact sheet was published in August 2026. All information is accurate as of date of publication. For further information please head to VALS website.

