

Legal Yarns

Online safety





What is online safety?

Online safety is the actions we can take to protect ourselves from harm and legal risk on the internet and social media.

Online safety includes:

- Managing our online activity, data and personal information so it is secure,
- Having strong privacy settings and passwords for our accounts,
- Having up-to-date software on our devices,
- Knowing how to protect ourselves from cyber-bullying and online sexual abuse
- Looking out for each other to protect each other from risks online.
- 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 and good online safety can protect you from those risks. 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. Looking out for each other online (see page 3)
2. Social Media and Young People (see page 4)
3. Privacy (see page 5)
4. Self-Incrimination (see page 7)
5. Cyber-bullying and Harassment (see page 8)
6. Sexual Abuse Online (see page 9)
7. Resources and Support (see page 10)

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





LOOKING OUT FOR EACH OTHER ONLINE

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

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

Online safety is a community effort – Technology changes quickly and it can be hard for some people to keep up with new information and to navigate new things. We need to help each other to understand online safety.

Young people, Elders and people with a disability may need extra help – Scammers target Elders and people with a disability to steal money, and young people are particularly vulnerable to online bullying, exploitation and abuse. Our Elders and people with disability may need support with digital literacy and to know what the latest scams are.

How do we look out for each other online?

As parents, family members, friends, teachers and carers, we must protect people in our communities from online harm by:

- **Learning** about what you can do to stay safe online and what the risks are online
- **Asking** each other what we know about online safety, bullying, abuse and scams
- **Teaching** each other how to use social media and the internet safely
- **Looking for signs** that someone is being scammed, threatened or bullied 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. For parents, it is very important to do this with your children, and to responsibly monitor how much your child is using the internet and what they are using it for.





SOCIAL MEDIA AND YOUNG PEOPLE

What's the social media ban for young people?

Children under the age of 16 are prevented from creating or maintaining accounts on certain social media platforms. The platforms include Snapchat, TikTok, Facebook, Instagram, X, Kick, Reddit, Threads, Twitch and YouTube.

The law was changed in December 2025, which means social media platforms ask your age when you sign up for an account and do not let you make an account if you're under 16. Platforms were required to "detect and deactivate or remove" accounts belonging to users they believe are underage. If you do still have a social media account, it could be removed or deactivated at any time before you turn 16 - even if you've already passed an age check.

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.

More information on the eSafety website, [here](#).

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. 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, but the social media platform could face penalties if they don't undertake steps to prevent use of underage accounts.

While you may not get in trouble for having an underage account, you still need to be careful about the other risks and harms involved in social media and internet use that we talk about in this Legal Yarn, including scams, bullying and sexual abuse.

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 with content online. There are apps that can support this, but open communication about expectations is important to keep children safe. We recommend that you try to:

- Look for signs of bullying and abuse online





- Monitor what and how often our young people engage online
- Talk about what you should do and should not do online
- Talk about the benefits of keeping yourself and your information offline
- Talk about what is illegal activity online
- Set expectations about staying safe online

Where can I find more information on the social media bans?

You can find out more information about social media restrictions through the [eSafety Commissioner website](#), which also has:

- [factsheets about the social media restrictions](#); and
- [deadly First Nations resources](#).

PRIVACY

How does being online impact my privacy?

Being online can impact your privacy and control over your information.

If you share your information publicly online, other people can use it and share it without your permission. People may still be able to access your information even if you deleted 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 screenshot or save posts and photos and reshare these without your permission.

How do I protect 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.

- Be careful about what you post and share online in the first place. Ask yourself: Do I need to share this? Is it safe to share this? Could this come back to bite me?
- Have a private, rather than public account





- Only accept friends and followers that you know personally and that you trust
- Block fake accounts
- Block people who make you feel uncomfortable or confused
- Do not give your personal information to anyone on social media
- Use strong privacy settings on your accounts.
- If you are not sure about sharing something, check with a trusted adult.

What is a fake account?

A fake account is an account pretending to be a person. They might be an AI bot or 'internet troll'. People and companies often use fake accounts for different reasons including:

- to scam you, steal your money and/or your identity,
- to spread hate and propaganda that supports their interests,
- to bully, harass and troll people without being identifiable.

Police also use fake accounts to monitor suspected criminal activity. 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.

How can I protect myself against fake profiles and accounts?

Fake accounts might want to add you as a friend on social media. Do not accept friend requests from people you don't know. To learn more about identity theft and scamming, read our [Legal Yarn on Identity Theft and Scams](#).

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?

Yes, but only if they have a warrant or believe you have committed a serious crime and there is evidence of that crime on your device.

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.

Can police access the data on my seized device?

Sometimes.

Police only can access the data from a confiscated device if:

- They have a warrant to access the data; or
- If a person is suspected of serious matters relating to terrorism or child exploitation – in this case the person may be required to give the police access to their device; or
- If the owner of the device gives them permission and access. Police may ask for a person for permission to look through their device or ask them to unlock the phone. The police may present these requests as co-operative or informal.

You do not need to give permission for police to access your data if they do not have a warrant and if you are not accused of terrorism or child exploitation, 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?

Probably.

It is very common for schools and employers to have the right to monitor your activity on devices, networks and internet servers that they provide through their “acceptable use policy” and contracts, policies, terms and conditions that you agree to. 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?

Be careful about what you do online – make sure you don't link yourself to criminal activity.

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.

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

YES, if:

- The image or video involves people under 18 – Sexting can be a crime if it involves people under 18, even if the underage person is sharing an image of themselves or said it's OK to share the image; or





- The person in the image or video does not consent to it being shared
 - Sharing an intimate image or video of someone without their consent is image-based abuse and is a crime.

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 nudes, sexual images or videos of yourself?

YES – If you are under 18 years old, 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.

It is not illegal if you are over 18, but it involves significant risks. You should try not to include your face in images to protect your privacy.

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:

- tell an adult you trust,
- ask a lawyer for help – see our number below
- report it to police.

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





Where can I get help?

Call us at VALS on 1800 064 865 or check out [our website](#) for more information or legal support.

The [eSafety Commissioner's website](#) also includes information on Online Safety.

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.

