



Staying safe in a connected world

Technology-facilitated abuse (TFA) is a growing form of harm in relationships, where online platforms and everyday technology are used to monitor, control or intimidate.

The 7 R's for staying safe

Technology can help us stay connected, informed, and safe. It plays a valuable role in everyday life by helping people communicate, work, learn, and access support. It can also be misused to monitor, control, intimidate, and harass. When used abusively, it can extend patterns of power and control into almost every part of a person's life. White Ribbon Australia's 7 R's offer a practical way to think about digital safety and respond early.



Understanding technology-facilitated abuse

Technology-facilitated abuse is not always a series of isolated incidents. It can form part of coercive control, where digital tools are used to monitor, pressure, isolate, threaten or dominate someone over time. It can happen through phones, apps, online accounts, social media, shared cloud services, smart home devices, wearables, cars, and tracking tools.

Why this matters

Research shows that

- 1 in 2 Australian adults have experienced at least one form of technology-facilitated abuse in their lifetime. Common forms include harassment, monitoring and control, emotional abuse and threats, and sexual or image-based abuse.
- Overall, 25% of children aged 10–17 have experienced non-consensual tracking, monitoring or harassment at some point, and 16% in the past 12 months.

* excludes ordinary parent or caregiver safety monitoring where the child was comfortable with it.

1. Respect

Respect means understanding that safety, privacy and consent matter online just as much as they do offline.

In healthy relationships, people do not demand passwords, insist on constant location sharing, pressure someone to hand over their phone, or tell them what they can post. Research found that 23.3% of Australians agreed it is reasonable to expect access to a partner's device codes, and 13.6% agreed it is reasonable to be able to track a partner whenever they want. Those attitudes can normalise control.



**RESPECT
PRIVACY**



**RESPECT
BOUNDARIES**



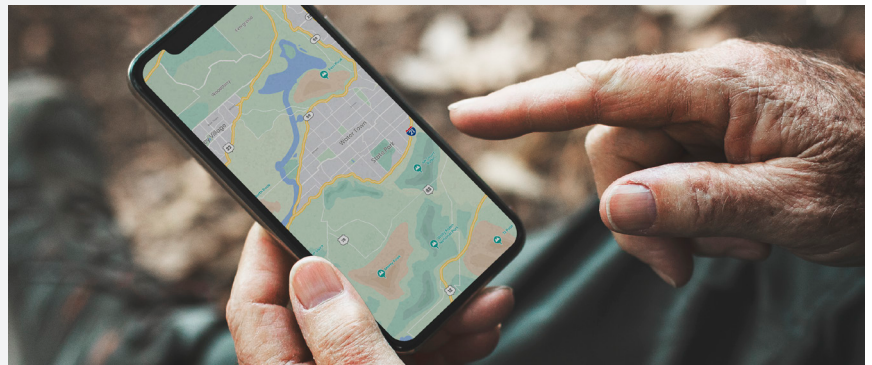
**RESPECT
CONSENT**

It is not respectful to:

- Demand passwords or passcodes
- Expect live location access at all times
- Pressure someone to share intimate images
- Monitor messages, social media or who someone speaks to
- Check a person's phone "to prove trust"

2. Recognise

Recognise when technology is being used as part of coercive control. Warning signs can include tracking, password pressure, constant checking, monitoring messages, threats, or misuse of connected devices.



19% of Australian children aged 10–12 have experienced non-consensual tracking, monitoring or harassment, and **14%** have experienced it in the past 12 months.

26% of Australian children aged 13–15 have experienced non-consensual tracking, monitoring or harassment, and **19%** have experienced it in the past 12 months.

Technology-facilitated abuse can take many forms, including,

- A need to know where you are all the time
- Checking your phone, messages or socials without permission
- Flooding you with calls or texts and gets angry if you do not reply
- Knowing things about your movements they should not know
- Using apps, devices or accounts to watch, track or frighten you
- Threatens to post, send or share private images

Some monitoring may be appropriate for safety, for example, by parents, carers, or during a genuine risk.

3. Review

Review your devices, apps, accounts and home tech for signs of ongoing access or monitoring.

Regularly check who has access to your accounts, what devices are connected, which apps can use your location, and whether shared albums, calendars, cloud backups or family-sharing tools are still active. Ensure you check privacy settings across devices and apps, and if safe to do so, disable location services. Please note that Bluetooth can be used to track location in some circumstances.



Technology leaves a digital trail, which is why reviewing device safety matters.

Review:

- Location sharing on your phone and apps
- Who can see your posts and stories
- Shared cloud accounts, photo streams and calendars
- Linked smart watches, tablets, cars and home devices
- Followers, contacts and account recovery details
- Login history and connected devices where platforms allow it.

4. Remove

Remove unsafe access where it is safe to do so.

That can mean removing unknown devices from your account, deleting old, shared accounts, logging out of prior sessions, removing unknown and unwanted followers, or uninstalling apps you do not use. But evidence matters. It is important to preserve evidence first, because once content is deleted or a person is blocked it can become harder to show what happened. Save screenshots, usernames, URLs, profile links, dates and times before making major changes.

If it is safe:

- Remove people from shared accounts and location sharing
- Clean up followers, contacts and permissions
- Uninstall apps you do not trust
- Take screenshots first
- Save usernames, links and dates
- Remove unknown devices and sessions

Safety note

If you believe someone may be using technology to monitor or control you, sudden changes can sometimes alert them. Consider making a safety plan first, using a safer device to seek advice, and alert your support network of your intentions.



5. Refuse

Refuse requests that cross your boundaries.

You do not have to share passwords, live location, account access or intimate images to prove trust. These demands can be part of coercive control, especially when they are used to pressure, monitor or isolate you. Refusing to give someone control, is part of being digitally safe. If someone is threatening to share intimate images or blackmailing you, do not send any further content and do not pay any money. If it is safe, stop engaging and end contact. Keep any evidence and seek support as soon as you can. The eSafety Commissioner can help with adult cyber abuse, image-based abuse and other online harm - www.esafety.gov.au



You can refuse:

PASSWORD SHARING

"I'm trying to keep all my accounts more secure, so I'm not sharing passwords anymore."

DEMANDS TO HAND OVER YOUR PHONE

"I'm not comfortable handing over my phone."

"PROOF" PHOTOS

"I'm not comfortable with that."

PRESSURE TO SEND INTIMATE IMAGES

"I don't share private images."

24/7 LOCATION ACCESS

"I'm turning off location sharing because I want more privacy."

REQUESTS TO DELETE EVIDENCE BEFORE YOU GET HELP

"I need to keep that for my own information."

6. Restrict

Restrict what others can access.

Strong passwords, different passwords for different accounts, multi-factor authentication, private account settings, and limiting location sharing all reduce risk.

It is always recommended to have strong passwords or passphrases, using different ones for each account, enabling multi-factor authentication where possible, and considering whether location services and geotagging should be switched off.

Restrict access by:

- Regularly changing passwords and using unique passphrases
- Turning on multi-factor authentication
- Setting accounts to private where possible
- Limiting who can message, tag or follow you
- Turning off location sharing and geotagging if safe
- Checking app permissions for camera, microphone, contacts and location



7. Reach out

Reach out early. If what is happening feels persistent, controlling or designed to make you afraid, it may be part of coercive control. You do not need to wait for physical violence to seek help. Support is available.



Support can come from a trusted friend, family member, school wellbeing staff, workplace contact, specialist service, eSafety or police. **1800RESPECT** is Australia's national domestic, family and sexual violence counselling, information and support service, available 24 hours a day, 7 days a week by phone, text, online chat and video call. The eSafety Commissioner can help with adult cyber abuse, image-based abuse and other online harm, and says to report threats to police. If you are in immediate danger, call **000**.

Getting support:

- Gather information, talk to someone you trust, or use a safer device to contact support.
- Call 1800RESPECT (1800 737 732) - 24-hour counselling, information and support. Also available via online chat and text options through the service website.
- Contact the eSafety Commissioner - www.esafety.gov.au, to help with adult cyber abuse, image-based abuse, online safety information and reporting pathways.
- Contact police, legal or specialist domestic and family violence support if there are threats, stalking, tracking or fear for your safety

Checklist

Use this list to review what and who has access to your information, location, accounts, and home technology. Not every item will apply to every person.

Apps

- ☐ Messaging and chat
- ☐ Social media
- ☐ Email
- ☐ Photo, file and cloud storage
- ☐ Maps, ride-share and travel
- ☐ Banking and payment
- ☐ Dating
- ☐ Family sharing or parental control
- ☐ Smart home and security
- ☐ Remote access, device management or monitoring
- ☐ Bluetooth or tracker
- ☐ Childcare, school
- ☐ Any app with access to location, camera, microphone, contacts, photos or Bluetooth

Accounts

- ☐ Primary email account
- ☐ Apple ID, Google account or other main device account
- ☐ Social media accounts
- ☐ Messaging accounts
- ☐ Cloud storage and photo backup accounts
- ☐ Banking and payment accounts
- ☐ Phone provider account
- ☐ Retail, delivery and online shopping accounts
- ☐ Streaming accounts
- ☐ Work, school or study accounts
- ☐ Government service accounts
- ☐ Password manager account
- ☐ Shared family accounts, calendars, albums or backups

Devices

- ☐ Phone or mobile device
- ☐ Tablet or iPad
- ☐ Laptop or desktop computer
- ☐ Smartwatch or fitness tracker
- ☐ Bluetooth trackers or item finders
- ☐ Car infotainment system, connected car app or digital keys
- ☐ Smart TV, streaming devices and game consoles
- ☐ Smart speakers or voice assistants
- ☐ Home security cameras, video doorbells and baby monitors
- ☐ Smart locks, intercoms, lights, plugs, thermostats and hubs

Checklist

What to check

- ☐ Who can see your location, posts, stories, photos and files
- ☐ Which devices are signed in to your accounts
- ☐ Account recovery email addresses and phone numbers
- ☐ Shared calendars, albums, notes and file folders
- ☐ Bluetooth pairings and tracker permissions
- ☐ Login alerts and sign-in history
- ☐ Followers, contacts and linked family members
- ☐ Whether old cloud accounts are still syncing data
- ☐ Whether cars, smart home devices or cameras are still shared
- ☐ Whether there are unknown apps, services, or devices you do not recognize.

Wi-Fi and home network

- ☐ Router or modem admin login
- ☐ Wi-Fi network name and password
- ☐ Guest network settings
- ☐ List of devices currently connected to Wi-Fi
- ☐ Old devices that should no longer have access
- ☐ Router firmware and software updates
- ☐ Remote management settings
- ☐ Any shared access to smart home hubs or security systems
- ☐ Lights, plugs, thermostats and hubs

For further resources and practical information, please visit,

- **White Ribbon Australia Online better guide**
- **eSafety Commissioner – www.esafety.com.au**
- **1800 Respect – www.1800respect.org.au**
- **Protective Group – www.protectivegroup.com.au**

And keep an eye out for upcoming White Ribbon Australia's Tech Facilitate Abuse training programs for workplaces and communities.

References

- 1800RESPECT. (n.d.). Device safety. <https://1800respect.org.au/help-and-support/technology-and-safety/devices>
- 1800RESPECT. (n.d.). Online accounts and app safety. https://1800respect.org.au/help-and-support/technology-and-safety/general_online_safety
- 1800RESPECT. (n.d.). Technology and safety. https://1800respect.org.au/help-and-support/technology-and-safety/online_safety_tips
- 1800RESPECT. (n.d.). 1800RESPECT. <https://1800respect.org.au/>
- eSafety Commissioner. (2023, December 22). How to collect evidence. <https://www.esafety.gov.au/report/how-to-collect-evidence>
- eSafety Commissioner. (2025, March 26). Collecting evidence safely. <https://www.esafety.gov.au/key-topics/domestic-family-violence/collecting-evidence-safely>
- eSafety Commissioner. (2025, December 2). Online safety checklist. <https://www.esafety.gov.au/key-topics/domestic-family-violence/online-safety-checklist>
- eSafety Commissioner. (2025, December 2). Tech-based domestic and family violence. <https://www.esafety.gov.au/women/reduce-technology-facilitated-abuse>
- eSafety Commissioner. (n.d.). Report online harm. <https://www.esafety.gov.au/report>



Get in touch

T 08 6370 0300

E info@whiteribbon.org.au

W www.whiteribbon.org.au

P PO Box 730, Cannington, WA 6087



@whiteribbonaust



@whiteribbonaustralia



@whiteribbonaust

White Ribbon Australia acknowledges Aboriginal and Torres Strait Islander peoples as the First Peoples of this land, and recognises their continuing connection to Country, culture, and community. We pay our respects to Elders past and present, and extend that respect to all First Nations peoples.

We also acknowledge victim-survivors of violence and abuse. We honour your strength, listen to your experiences, and recognise the impact violence has on individuals, families, and communities. We are committed to prevention, accountability, and creating safer, more respectful futures for everyone. accountability, and creating safer, more respectful futures for everyone.

 **White Ribbon
Australia**