E-Safety Checklist

Adapted with thanks from *Northern Territory Domestic and Family Violence Risk Assessment and Management Framework,* and the e-Safety Commissioner *Tech-based domestic and family violence* resources.

Domestic and family violence is characterised as any behaviour or any pattern of abusive behaviours that is designed to control or intimidate the victim-survivor. Rather than as an incident or series of incidents of abuse, DFV is distinguished by an underlying pattern of power and control by one person over another, often described as coercive control.

People using violence might use digital technology to facilitate their violence behaviours. as part of their abusive behaviour. This is commonly referred to as technology facilitated abuse, and is a key part of how coercive and controlling behaviours are used against victim-survivors.

Technology-facilitated abuse can be difficult to spot because the behaviours are often subtle, targeted and embedded within everyday technology use. Victim-survivors may not recognise they are being monitored or controlled through technology.

Common signs of technology-facilitated abuse

- Sending repeated abusive, threatening or unwanted messages or calls.
- Tracking a victim-survivor's movements.
- Checking who victim-survivor talks to online or over the phone.
- Creating fake social media accounts or posting harassing content about the victim-survivor.
- Controlling or taking over online accounts or locking the victim-survivor out of accounts such as Wi-Fi, email, social media or banking.
- Making, sharing, or threatening to share intimate images or videos without consent (also known as 'intimate-image abuse'), including through the use of Artificial Intelligence (AI).
- Using cameras or recording devices to spy on the victim-survivor, including in their own home.
- Using smart home devices to monitor the victim-survivor, or restricting access to that technology to control the victim survivor. These can include:
  - Smart doorbells, locks or lights
  - Virtual assistant technology
  - Robot vacuum cleaners
  - Pet or baby monitors
  - Home appliances that can be controlled outside the home, such as air conditioners, TVs, speakers, and refrigerators.
  - Bluetooth and internet enabled medical devices.

Signs of monitoring

- The person using violence seems to know the victim-survivor's location or where they have been. GPS tracking devices are easily available and can be hard to see. Other technology, such as mobile phones or smart watches can be used to track location, movements and to record conversations.
- The victim-survivor has noticed strange or unusual activity on their phone.
- The person using violence has access to the victim-survivor's mobile phone, social media accounts, bills or passwords.
- The person using violence knows what the victim-survivor is doing when they are home alone.
- The victim-survivor experiences unusually fast battery drain or increased data usage on their phone. This can indicate that spyware is operating on the device. Spyware can also be installed on home computers, tablets, and smart devices to monitor activities, locations and who the victim-survivor is communicating with.

When monitoring is suspected

Workers should carefully consider the potential risks or repercussions of removing a suspected monitoring device, and safety plan with the victim about these risks.

While victim-survivors often want to remove the technology being used against them, doing so may escalate the controlling behaviour if the person using violence perceive a loss of control. At the same time, the current risks of monitoring may be so high that immediate actions are required to limit the PUVs access to the victim-survivor.

In some situations, an option could be for the victim-survivor to continue using the monitored device while accessing a separate safe device device for safety planning and sensitive communications. This requires careful and deliberate planning in partnership with the victim-survivor.

Actions to increase e-safety

Workers can support victim-survivors to improve their safety by:

- Making sure the victim-survivor is aware that hidden cameras may be installed in their home and may be accessed remotely, and that device cameras may be accessed remotely through spyware on phones, tablets or computers.
- Encourage the victim-survivor to trust their instincts. If they suspect they are being monitored, stalked or harassed through technology, this concern should be taken seriously.
- Talking with the victim-survivor and people close to them, including children, about online safety and location sharing risks.

Check devices are secure

Video tutorials are available on the e-Safety Commissioner webpage on how to undertake a number of these tasks on different devices.

Support victim-survivors to:

- ☐ Turn off location sharing where safe to do so. This may also need to include social media (e.g., Instagram, Snapchat, Strava).
- ☐ Disable password saving and automatic sign-in features.
- ☐ Access, manage and delete their browsing history if safe to do so. Alternatively, show the client how to use the 'private browsing' function on their devices.
- ☐ Create a new email and social media accounts without identifying information.
- ☐ Review and strengthen online privacy, including 'blocking' others, including people who 'report' information back to the PUV.
- ☐ Learn how to sign out of accounts completely.
- ☐ Check for unusual apps on theirs/their child's phone and to remove them if safe to do so.

- ☐ Enable automatic screen locking using a secure PIN or passcode on all devices.

Check online accounts are secure

Support victim-survivors to:

- ☐ Change passwords and PINs using a safe device. Consider using a secure password managing application or secure 'Passkeys'.
- ☐ Avoid using cloud-based password managers as they may be used to automatic sign in to online accounts
- ☐ Enable multi-factor authentication or two-step verification where possible. This is an extra security measure that asks for a security code that is sent via email or mobile.
- ☐ Use the Arc App to collect and store evidence of DFV safely: https://arc-app.org.au.
- ☐ Avoid using their device or email for account password recovery. Ensure recovery methods are secure and the person using violence does not have access before making changes.

Communicate safely

Support victim-survivors to:

- ☐ Consider using their own prepaid or private mobile phone rather than a phone linked to the person using violence.
- ☐ Avoid transferring their old SIM card into a new phone.
- ☐ Handwrite important contact numbers and manually enter them into a safe phone.
- ☐ Use airplane mode to reduce the risk of being tracked.
- ☐ Use encrypted messaging apps, such as Signal or WhatsApp, for sensitive communication.
- ☐ Regularly clear browsing histories and chat histories where it is safe to do so.

Important information about AusAlert

Australia's new national warning system, **AusAlert**, will be operational in 2026. The system uses the latest technology to send emergency messages to compatible mobile devices during disasters such as bushfires, severe weather and public health emergencies.

Some emergency alerts cannot be turned off.

If receiving an AusAlert could compromise a victim-survivor's safety, consider keeping the safety devices turned off or in airplane mode when not in use. Remember that Wi-Fi can usually still be accessed in airplane mode.