Protecting clients from technology-facilitated abuse

A guide to support clients **who've just left their abuser**

Client profile

- Has left their abuser and in the process of moving to a safe location
- Safety is dependent on their abuser not knowing their new safe location

Goal

- Safeguard their immediate physical safety, as well as the safety of any children in their care
- Reduce the risk that technology can be used to track them or their new location

Objectives

- Help them understand how technology can be misused by an abuser
- Help them access a safe phone or safe device
- Agree on appropriate, short-term restricted technology use for themselves and any children in their care
- Make a time to discuss how they can reconnect with technology and devices safely

Key safety requirements for frontline workers to consider

- Any technology safety planning is done in the context of broader domestic, family and sexual violence risk assessment and safety planning tools.
- eSafety recommends steps **5 and 6** are done **after your client has left their abuser** but **before they reach their new safe location**.
- Please be aware their abuser might be alerted to changes made to their (or any children's) devices or technology.

7 technology safety steps to work through with clients

1. Explain the role of technology-facilitated abuse

- When digital technology (the internet, devices, smart technology) is used to harm or abuse someone, it's called 'technology-facilitated abuse' or '**tech-based abuse**'.
- This form of abuse occurs in most cases of domestic and family violence.
- This form of abuse can be covered by court orders, such as an Apprehended Domestic Violence Order.
- The abuse includes controlling the use of someone's technology and devices and using technology to scare or shame them.
- Some types of abuse are more obvious, such as **harassment, threats, impersonation**.
- Some types of abuse are more hidden, such as **surveillance and tracking**.
- Children's devices can also be used to track and cause harm – for example using tracking apps on phones or tablets, or cameras in toys.

2. Help them access a safe phone or safe device for sensitive communication

A safe device is:

- new (**Wesnet provides new phones via the Safe Connections Program**), or borrowed from a trusted person and is a device their abuser has never accessed
- not linked to or backed up by an existing device
- not linked to any current iCloud, Google, Outlook or other online accounts.

Before using a safe device, recommend:

- turning off **bluetooth, wi-fi auto connect and location services**
- downloading a subscription-based VPN ('**virtual private network**') before using wi-fi.

There are other options if accessing a safe device is not possible:

- Reset current device to factory settings.
- Use a work computer (if it's safe to do so) or go to a library or a trusted person's place to use their computer.

Across all devices, recommend they browse in **incognito** or InPrivate mode and log out of any online accounts they have logged into.

3. Recommend these steps to prevent harassment via text, phone and social media on their new safe phone:

- Set up a new number with a new SIM on the safe phone.
- Set caller ID to private.
- If appropriate, block the number of the abuser.
- If appropriate, also block or silence unknown callers (callers with no caller ID) – this is an option on most phone services.
- If access to social media is needed, **change all accounts to a new password or a passphrase** (which is more secure) and then block the abuser.

4. Identify devices they want to take with them, including children's devices

Focus on:

- Mobile phones
- Tablets
- Laptops
- Smart watches
- Smart toys
- Baby monitoring devices
- GPS systems in the car

5. Discuss temporarily turning off all smart devices to reduce the risk of being tracked via spyware. If not possible, recommend they turn off:

- location settings
- cellular data
- wi-fi
- bluetooth.

Reassure them this is a short-term measure by saying things like:

- 'We want to make sure your abuser cannot track you and your new safe location.'
- 'If you decide to limit any technology use, this is a short-term measure only – we know how important technology and devices are to your every-day life.'
- 'If possible, let's apply the same limits to any devices and smart toys used by children in your care.'
- 'We'll work with you to make a plan to use technology safely once you've safely left your abuser'.

6. Recommend they search for any tracking devices (such as AirTags) in any luggage and their car. If they find any, suggest they leave the tracker(s) at a location far from their new safe location.

7. Make a time with your client to review their devices, accounts and apps comprehensively to support safe technology use.

Need help to support your client?

Request a call back from eSafety's Technology-Facilitated Abuse Support Service via the **enquiry form**.

For resources and online safety advice, visit: **eSafety.gov.au/TFA-support-service**