Protecting clients from technology-facilitated abuse

A guide to support clients being digitally harassed or tracked by their abuser

Client profile

- Has left their abuser
- Continues to be harassed and/or tracked by their abuser, even though they have taken steps to secure their online and digital safety
- Is afraid for their safety and the safety of children in their care

Goal

- Limit their abuser's ability to digitally harass or track them or any children in their care
- Collect evidence of possible technology or device vulnerabilities to discuss with eSafety's Technology-Facilitated Abuse Support Service

Objectives

- Help them understand how technology can be misused by an abuser
- Turn off any location-tracking apps on their devices
- Identify possible suspicious devices or objects that could be tracking devices
- Help them access a safe phone or safe device

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.
- Any changes to technology and device use are only made after considering your client's specific situation and safety.

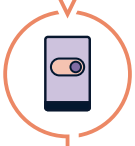
9 technology safety steps to work through with clients

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. Conduct a technology, device and account audit (Refer to: **Technology audit: Identifying a client's devices, apps and online accounts**).

3. Recommend covering any cameras on their devices with removable tape and turning off microphones, if possible.



4. Discuss temporarily turning off all smart devices to reduce the risk of being tracked via spyware.

If that is not possible, ask them to consider turning these off:

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

5. Document any signs that suggest a device has been infected with spyware.

Ask questions like these:

- 'Have you noticed any apps you don't remember downloading?'
- 'Have you noticed any double ups of everyday apps? For example, two of the calculator or calendar app?'
- 'Is the device slower than usual or taking a long time to load?'
- 'Has any device battery been draining faster than usual?'
- 'Has any device been switching itself off and on?'
- 'Have there been unexplained spikes in your data use?'
- 'Have apps, emails or messages disappeared mysteriously?'
- 'Have you been unable to call certain numbers or access certain websites?'

6. Document any signs of tech-based harassment or impersonation.

Ask questions like these:

- 'Is your abuser harassing you via phone, text, email, message, or social media?'
- '**What evidence have you collected**? Do you have any screenshots, URLs or voice recordings?'
- 'Are you aware of any social media accounts being used to discredit, harass or humiliate you? What evidence have you collected from these accounts?'
- 'Have you been unable to call certain numbers or access certain websites?'

7. Document other suspicious objects, activities or new technology.

Ask questions like these:

- 'Are you using any USBs or hard drives that your abuser may have had access to? If so, what devices are they and what computers have you plugged them into?'
- 'Have you found or seen any unusual objects in your wallet or bag? Where were they and what did they look like?'
- 'Have you checked your car on the inside and outside for any unusual objects? If you discovered something, where were they and what did they look like?'
- 'Thinking of any smart-home devices, have you noticed anything unusual? Lights turning on and off at odd times? Home alarms set off with no explanation?'
- 'Have you received any objects or gifts from your abuser? What were they and where are they now?'
- 'Have any children in your care received any new toys or devices from your abuser, their parents or other relatives of your abuser? If yes, what were they and where are they now?'
- 'Are you using pet monitors or baby monitors or security cameras that your abuser may have had access to? Has anyone installed cameras in places where you would expect privacy? When and where were those cameras installed?'

8. 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.

9. Request a call back from eSafety's Technology-Facilitated Abuse Support Service via the enquiry form to discuss next technology steps.

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