

Technology Audit

Identifying a client's devices, apps and online accounts

Key safety requirements

- Any technology safety planning is done in the context of broader family, domestic and sexual violence risk assessment and safety planning tools.
- Any changes to technology and device use are only made after considering a client's specific situation and safety.
- In some cases, it may be safest not to make any changes to a client's device or technology to avoid triggering further violence.

Using this auditing document

- This is not an exhaustive list. It includes examples of the more popular devices, apps and online accounts. We recommend asking clients to think about any other technology they use and is not listed.
- To help inform current and future safety planning, devices, apps and online accounts have been flagged when their settings and capabilities could be used by an abuser to track, coerce or harm a client. Specifically, the potential for:



tracking or geo-tagging, or logging other time and location-specific data



a mailing or home address is required



hosting sensitive or personal information



an in-built camera



connecting to wi-fi, bluetooth or GPS (device-level only)



spyware infection (device-level only)




































- These safety considerations should be used as a guide only.
- There is a column for the client to note whether the abuser had access to a particular device, app or online account, or is likely to have had access.
- If a client has any children in their care, we recommend doing a separate audit of their devices, apps and online accounts.
- We also recommend prompting clients to think about any work devices, apps or online accounts their abuser might have accessed.







Need help to support your client?

Request a call back from eSafety's Technology-Facilitated Abuse Support Service via the [enquiry form](#).

The TFA Support Service (the Service), and the information provided through it, are provided 'as is' (and as a guide only) and are not a substitute for professional advice (whether medical, clinical, legal, technical, or otherwise). You should not rely on the Service to make any decision, and you are encouraged to seek professional advice if appropriate. For more information about how the Service can be used, and its limitations, please read the full [Terms and Conditions](#).

Client technology audit

Category: personal devices		
Item	Safety considerations	Tick if abuser ever had access
<input type="checkbox"/> Laptops	    	<input type="checkbox"/>
<input type="checkbox"/> Mobile phones	    	<input type="checkbox"/>
<input type="checkbox"/> Mobility aids and assistive technology	    	<input type="checkbox"/>
<input type="checkbox"/> Tablets: iPad, Galaxy Tablet	    	<input type="checkbox"/>
<input type="checkbox"/> Fitness watches	   	<input type="checkbox"/>
<input type="checkbox"/> Smart watches	   	<input type="checkbox"/>
<input type="checkbox"/> Home modems	   	<input type="checkbox"/>
<input type="checkbox"/> USBs and portable hard drives	 	<input type="checkbox"/>
<input type="checkbox"/> Bluetooth headphones		<input type="checkbox"/>
Other:		<input type="checkbox"/>

	tracking or geo-tagging, or logging other time and location-specific data		a mailing or home address is required
	hosting sensitive or personal information		an in-built camera
	connecting to wi-fi, bluetooth or GPS (device-level only)		spyware infection (device-level only)

Category: location and travel

Item	Safety considerations	Tick if abuser ever had access
<input type="checkbox"/> Dashcams	    	<input type="checkbox"/>
<input type="checkbox"/> GPS devices: Garmin, Navman	   	<input type="checkbox"/>
<input type="checkbox"/> Pet microchip	   	<input type="checkbox"/>
<input type="checkbox"/> Tracking devices: AirTags/SmartTags/Tiles	  	<input type="checkbox"/>
<input type="checkbox"/> eToll and/or Linkt account	  	<input type="checkbox"/>
<input type="checkbox"/> Location-sharing apps: Life360, Findmykids, Pingo	  	<input type="checkbox"/>
<input type="checkbox"/> Ride-share and taxi accounts: Uber, DiDi, Ola	  	<input type="checkbox"/>
<input type="checkbox"/> Transport cards and accounts: Opal, Myki	  	<input type="checkbox"/>
<input type="checkbox"/> Bike/scooter sharing apps: Lime, Beam	 	<input type="checkbox"/>
<input type="checkbox"/> 'Find My Device' accounts	 	<input type="checkbox"/>
<input type="checkbox"/> Map apps: Google Maps, Apple Maps	 	<input type="checkbox"/>
<input type="checkbox"/> Parking accounts/apps	 	<input type="checkbox"/>
Other:		<input type="checkbox"/>



tracking or geo-tagging, or logging other time and location-specific data



hosting sensitive or personal information



connecting to wi-fi, bluetooth or GPS (device-level only)



a mailing or home address is required


















an in-built camera



spyware infection (device-level only)

Category: sensitive and personal information

Item	Safety considerations	Tick if abuser ever had access
<input type="checkbox"/> Cloud storage: iCloud, Google Drive, Dropbox, One Drive	  	<input type="checkbox"/>
<input type="checkbox"/> Health accounts/apps: HotDoc, Health Connect, Samsung Health	  	<input type="checkbox"/>
<input type="checkbox"/> Mobile phone accounts	  	<input type="checkbox"/>
<input type="checkbox"/> Government services accounts/apps: MyGov, Medicare, Centrelink, ATO, digital driver's license	 	<input type="checkbox"/>
<input type="checkbox"/> Online calendars: Google, Outlook, iCal, Samsung	 	<input type="checkbox"/>
<input type="checkbox"/> Email: Gmail, Outlook, hotmail		<input type="checkbox"/>
<input type="checkbox"/> Fitness accounts: Apple Fitness+, Google Fit, MapMyRun		<input type="checkbox"/>
Other:		<input type="checkbox"/>



tracking or geo-tagging, or logging other time and location-specific data



a mailing or home address is required



hosting sensitive or personal information



an in-built camera
















connecting to wi-fi, bluetooth or GPS (device-level only)


















spyware infection (device-level only)

Category: children

Item	Safety considerations	Tick if abuser ever had access
<input type="checkbox"/> Drones	    	<input type="checkbox"/>
<input type="checkbox"/> Baby monitors	   	<input type="checkbox"/>
<input type="checkbox"/> Smart toys, including voice command	   	<input type="checkbox"/>
Other:		<input type="checkbox"/>

Category: social media

Item	Safety considerations	Tick if abuser ever had access
<input type="checkbox"/> Facebook	 	<input type="checkbox"/>
<input type="checkbox"/> Foursquare	 	<input type="checkbox"/>
<input type="checkbox"/> Instagram	 	<input type="checkbox"/>
<input type="checkbox"/> Snapchat	 	<input type="checkbox"/>
<input type="checkbox"/> TikTok	 	<input type="checkbox"/>
<input type="checkbox"/> X (Twitter)	 	<input type="checkbox"/>
<input type="checkbox"/> YouTube	 	<input type="checkbox"/>
<input type="checkbox"/> Reddit		<input type="checkbox"/>
Other:		<input type="checkbox"/>



tracking or geo-tagging, or logging other time and location-specific data



a mailing or home address is required



hosting sensitive or personal information



an in-built camera







































connecting to wi-fi, bluetooth or GPS (device-level only)



spyware infection (device-level only)

Category: home and lifestyle

Item	Safety considerations	Tick if abuser ever had access
<input type="checkbox"/> Alarm systems	     	<input type="checkbox"/>
<input type="checkbox"/> Security cameras	     	<input type="checkbox"/>
<input type="checkbox"/> Gaming, including consoles, accounts, apps	    	<input type="checkbox"/>
<input type="checkbox"/> Virtual assistant: Google Nest, Amazon Alexa	    	<input type="checkbox"/>
<input type="checkbox"/> Any smart electronics: TVs, washing machines, kettles, speakers, vacuum	   	<input type="checkbox"/>
<input type="checkbox"/> Family Library	 	<input type="checkbox"/>
<input type="checkbox"/> Family Sharing	 	<input type="checkbox"/>
<input type="checkbox"/> Food delivery services: Uber eats, Door Dash, Menulog	 	<input type="checkbox"/>
<input type="checkbox"/> Grocery/supermarket/chemist accounts with delivery services		<input type="checkbox"/>
<input type="checkbox"/> MyPost account		<input type="checkbox"/>
<input type="checkbox"/> Online shopping accounts/apps with delivery services: clothing, beauty, accessories		<input type="checkbox"/>
<input type="checkbox"/> Utilities (electricity, internet, water, gas)		<input type="checkbox"/>
Other:		<input type="checkbox"/>



tracking or geo-tagging, or logging other time and location-specific data



a mailing or home address is required



hosting sensitive or personal information



an in-built camera



connecting to wi-fi, bluetooth or GPS (device-level only)








spyware infection (device-level only)

Category: finance

Item	Safety considerations	Tick if abuser ever had access
<input type="checkbox"/> Afterpay	 	<input type="checkbox"/>
<input type="checkbox"/> Insurance accounts (health, car, home)	 	<input type="checkbox"/>
<input type="checkbox"/> Investment apps/accounts (CommSec, Stake, Selfwealth)	 	<input type="checkbox"/>
<input type="checkbox"/> Online bank accounts (credit/debit cards)	 	<input type="checkbox"/>
<input type="checkbox"/> PayPal	 	<input type="checkbox"/>
Other:		<input type="checkbox"/>

Category: work and education

Item	Safety considerations	Tick if abuser ever had access
<input type="checkbox"/> Anydesk		<input type="checkbox"/>
<input type="checkbox"/> LogMeIn		<input type="checkbox"/>
<input type="checkbox"/> My Uni		<input type="checkbox"/>
<input type="checkbox"/> Shared working or learning accounts: Moodle, Blackboard		<input type="checkbox"/>
<input type="checkbox"/> Teamviewer		<input type="checkbox"/>
Other:		<input type="checkbox"/>



tracking or geo-tagging, or logging other time and location-specific data



a mailing or home address is required



hosting sensitive or personal information



an in-built camera



connecting to wi-fi, bluetooth or GPS (device-level only)



spyware infection (device-level only)