Technology Safety Planning Tipsheet

General Recommendations:

- Ensure your mobile phone and computer have anti-spyware & anti-malware software
- Change all passwords and PIN numbers, see the ***Creating Safe Passwords Tipsheet***
- Limit what you share online
- Educate your family, friends and work colleagues about what they share about you online
- Use a USB flash drive or external hard drive to back up:
    - Important documents;
    - Anything that you can use as evidence (E.g., screenshots of Facebook messages from the perpetrator, emails, etc.); and
    - Friends' email and contact information
        - You can download free apps and software to download this information from your phone or computer

Your Digital Footprint:

- Information you leave behind – everything you do online leaves a trace
    - **Assess what online information exists about you**
        - Do a Google search of yourself to see what information is available online so you know what precautions to take
        - You can set up a ***Google Alert*** with key words such as your name, email and phone number so if these are posted on the internet, you will be alerted
        - If you are concerned there are intimate images of you online without your permission and you have a copy of that image, you can search Google for matching images by going to www.images.google.com. Use the camera button to upload the image for the purpose of finding any matching images posted online
        - If you need your personal information or images removed from Google, you can request removal by visiting www.support.google.com/websearch/. Similarly, you can contact Microsoft using their online form to request images to be removed from Bing search results, OneDrive and Xbox Live (Google "Microsoft Report Content")
        - If there is a website where images of you are posted without your permission, you can contact the website's ***Webmaster*** directly to request the images be removed. To find out the Webmaster's details simply copy and paste the website URL into a "whois" search. E.g., whois.domaintools.com for international websites or whois.auregistry.net.au for Australian websites
    - **Online accounts with profiles or an online presence**
        - Change your email and passwords
        - Delete existing online accounts or update privacy settings, particularly it they contain large amounts of information or photos (E.g., Facebook, Instagram, etc)
        - Review who can access your information
        - On Facebook you can turn on alerts if someone accesses your account on a new computer or device
        - Turn off geolocations and tag suggestions
            - E.g., be aware Facebook Messenger has location settings on as a default and can provide a map of your location when you send a message
    - **Review all the privacy and security settings**
        - Change your settings to the highest possible privacy and security

- **Avoid public forums such as Reddit**
  - Perpetrator can see your posts
  - Can be an avenue of bullying and harassment

Spyware:

- Apps or software that can be download onto a person's mobile phone or computer to collect information about them, monitor their movements, private calls, messages, emails etc.
  - Spyware requires an internet connection to function – disconnect your computer or mobile phone from the internet
  - Factory reset the computer or mobile phone – this is the most effective method of getting rid of spyware
  - Use spyware detection/removal software
  - Install anti-spyware software
    - E.g., Windows Defender (PC), Avira Free Antivirus (Mac)
  - Be extremely careful about opening .exe files or attachments, pictures or cartoons in emails

Mobile Device Precautions (Mobile device: mobile phones, iPads, tablets):

- Set a PIN to lock your mobile device
- Secure your Google or iCloud account
- Install anti-spyware apps/software
- Immediately change your password for your mobile phone account
- Delete apps that you do not use
- Review apps to see if they have any features that could be used to give away your location or leak information about you; e.g. switch of location tag on Facebook Messenger
- Learn to turn off wi-fi, GPS and geolocation services; change the default so that your location tags aren't added to photos, see SmartSafe videos for help: www.smartsafe.org.au
- Check to see if mobile phone is 'jailbroken' or 'rooted. See www.lookout.com
- Be aware of children's devices, eg tablets or smartphones
- Fight fire with fire! If you don't want to get rid of your smartphone, you can download apps to assist with your safety. Search for these Apps for your iPhone/Android:
  - Evidence collecting – see www.plus.smartsafe.org.au
  - Hide incoming text messages and phone calls – iPhone: 'CoverMe Private Texting', 'Secure Phone Calls'; Android: 'Hide My Text'
  - Back up apps – allows you to back up selected apps and their settings so if you do a factory reset you can get back your favourite apps
  - Back up contacts – sends your contacts list to your email that can be restored onto your phone or a new device; contacts list can also back up to iCloud or Google
  - Back up voice messages – allows you to backup voice mail messages onto your computer if you need them for evidence. E.g., iExplorer or Audacity
  - Panic alarms – text your location to designated contacts. iPhone/Android: 'The Panic Button', 'Red Panic Button'
  - Hide caller ID –useful if you change your phone number so that when you make a call the person receiving to call cannot identify your number
  - 'Aurora' and 'Daisy' – domestic violence apps (iPhone/Android) with service contacts
- If someone has given your client a mobile phone it is best to do a factory reset to ensure there is no malicious software on it

Computer Precautions:

- Set up a password to access your computer, see the **creating safe passwords tipsheet**
- Be aware that **all saved usernames and passwords** can be **accessed and viewed on most browsers**
- Be careful as information can be synced across the same browser on different devices

- Be aware of passwords being saved in browsers and having connected logins with other websites
    - E.g., Gmail, Google Search and Youtube (owned by Google) are linked;
- Be aware if you use Apple devices, they can be synced. E.g., iMessages can be sent to a laptop
- Be aware Apple devices have inbuilt GPS tracking ('Find my Phone') - this is accessed through iCloud
- Do not save your password and user information in the browser. Do not tick 'Remember my password on this computer' when at risk
- Regularly clear your browsing history – clients may want to delete specific entries rather than clear the entire history if that could raise suspicions
- Use private browsing so that web history of pages visited is not logged – E.g., Chrome (Incognito); Internet Explorer (InPrivate); Mozilla Firefox and Safari (Private Browsing)
- Regularly clear Google search history. Go to: www.google.com/searchhistory → 'Settings' button → Remove Items
- Consider setting up new email accounts, set up on a safe computer. It can be helpful to make multiple email accounts so that if any are hacked you can pinpoint which account has been accessed. E.g., separate accounts for:
    - Friends/family
    - Social media accounts
    - Online registrations
    - Finances

Gathering evidence:

- Do not delete text messages, voicemail messages, photos
- Try and save any evidence to a computer/USB flash drive
- Use screenshots (see www.take-a-screenshot.org) and save the image as the date & time it was taken. If taking screenshots of websites, always include the URL in the screenshot
- Keep a diary or voice notes of incidents including dates and times
- Consider giving police written permission to access your phone, computer, Facebook, email account etc. if a matter is being investigated

Get legal advice!

- Contact your local Women's Legal Service:
    - **NSW** - Women's Legal Services NSW: www.wlsnsw.org.au
    - **VIC -** Women's Legal Service Victoria: www.womenslegal.org.au
    - **ACT** - Women's Legal Centre: www.womenslegalact.org
    - **QLD** -
        - Women's Legal Service Queensland: www.wlsq.org.au
        - North Queensland Women's Legal Service: www.nqwls.com.au
    - **NT** -
        - Central Australian Women's Legal Service: www.cawls.org.au
        - Katherine Women's Information and Legal Service: www.kwils.com.au
        - Top End Women's Legal Service: www.www.tewls.org.au
    - **TAS -** Women's Legal Service Tasmania: www.womenslegaltas.org.au
    - **SA -** Women's Legal Service (SA): www.wlssa.org.au
    - **WA -** Women's Law Centre of WA: www.wlcwa.org.au
- Contact your local Community Legal Centre, to find your local centre, visit www.naclc.org.au/directory