**[Insert organisation name/logo]**

# [insert organisation name] COMPUTER aND PHONE USE GUIDELINES

***Note\****
*This is a general guide for organisations where devices made available for shared use by clients and/or a landline. If not relevant for your organisation, please ignore or adjust to suit.*

*\*Please delete note before finalising this template.*

These guidelines relate to client use of **[insert organisation name]**’s computers and phones (devices’). Staff will communicate these guidelines to clients during orientation and as required. Staff will ensure that the devices provided by the organisation are equally accessible to everyone in the service.

1. **Online safety**

To ensure **[insert organisation name]**’s devices and systems are kept secure, all devices have automatic updates and must be updated when prompted. In addition, for your own cyber security, clients are advised to:

* Turn on multi-factor authentication (MFA) starting with most important accounts (email, online banking and accounts with stored payment details, social media)
* Back up your personal devices
* Change your passwords to secure pass phrases (long, unpredictable, unique). (Considering using a password manager if you are unable to remember all your passwords/pass phrases)
* Watch out for scams emails and text messages

More information can be found [here](https://www.cyber.gov.au/protect-yourself/easy-steps-secure-yourself-online)

1. **Monitoring**

**[Insert organisation name]** regularly monitors the use of all devices, in particular websites visited by clients to ensure the safety and security of clients and **[insert organisation name]** and its staff.

1. **Email use**

Clients do not have access to an **[insert organisation name]** email address. If an email address needs to be created, it can be done so through a free provider (e.g. gmail)

1. **Landline use**

*If relevant*, clients may use **[insert organisation name]**’s landline phone to make telephone calls which relate to their individual treatment plan.

1. **Personal device/mobile phone use**

*If relevant,* clients may use their own personal devices as required, within reasonable expectations, ensuring this does not interfere with following **[insert organisation name]**’s program.

1. **Confidentiality and privacy**

**[insert organisation name]** ensures the confidentiality and privacy of its clients is strictly maintained. Clients are prohibited from disclosing information or sharing photos of others within **[insert organisation name]** without their consent.

1. **Prohibited use**

The **[insert organisation name]**’s devices should not be used for:

* crime-related activities
* gambling
* pornography
* racism, homophobia or vilification (e.g. in games, emails, etc.)
* harassing, intimidating, stalking or threatening someone
* illegal use of copyright material

The **[insert organisation name]**’s devices should not be used to:

* download software (e.g. download from the internet or a USB) without prior agreement from **[insert organisation name]**
* download very large files or access streaming audio or video without prior agreement from the **[insert organisation name]**
* change the settings, passwords, folders etc. on shared devices
1. **Non-compliance of guidelines**

Depending on how these guidelines have not been followed, **[insert organisation name]** staff may need to provide you with a warning of potential outcomes or restrict your access to devices.