

Guidelines for Computer, Internet, Email and Phone Use

1. Overview of the Guidelines

The guidelines relate to personal use of [insert organisation name] computers and phones by consumers, carers, volunteers, students, staff and board members of [insert organisation name].

2. Considerations

Consumers, carers, Board members, employees, students, and volunteers will comply with all laws when using [insert organisation name] computers and phones.

Using [insert organisation name]'s computer or phone resources to seek out, access or send any material of an offensive, obscene or defamatory nature is prohibited and may result in:

- withdrawal of permission to use [insert organisation name]'s computers and phones for consumers and carers;
- disciplinary action for Board members, employees, students, and volunteers.

Consumers and Carers:

Consumers and carers may use computers and phones which have been dedicated by the organisation for consumer and carer use.

The aim is to ensure, as far as possible, these phones and computers are equally accessible to all consumers and carers.

Board members, employees, students, and volunteers

All Board members, employees, students, and volunteers will use communication systems and equipment provided by the organisation only for the purpose of fulfilling [insert organisation name]'s mission, unless authorised otherwise by [insert position].

3. Guidelines – Consumers and Carers

3.1 Computer Use

Booking Computer Time

Computer use may be booked in advance, or (if available) on the spot, for a period of up to **[insert time]**, using the computer booking sheet. Consumers and carers will finish computer use on time.

Computer Rules

Staff will take all appropriate steps to inform and educate consumers and carers about the Computer Rules (Appendix 1) and to implement them.

The Computer Rules are placed in areas where consumers and carers will be using computers.

Computer Monitoring

[insert organisation name] monitors logs of internet usage which may reveal information such as which servers (including websites) have been accessed by the user and email addresses used.

3.2 Email Use

Consumers and carers do not have access to an **[insert organisation name]** email address. If an email address needs to be obtained, it will be done so through a free provider (e.g. gmail, hotmail)

3.3 Phone Use

Consumers and carers may use a landline phone to make telephone calls which relate to individual support plans.

Mobile Telephones

Consumers and carers do not have access to **[insert organisation name]** mobile phones.

3.4 Monitoring Activities

Staff may maintain an awareness of the types of activities for which consumers and carers are using computers and phones.

4. Guidelines – Board members, employees, students, and volunteers

4.1 Email Use

Employees, Board members, volunteers and students may use email access provided by the organisation for any work-related purposes of **[insert organisation name]**.

With permission from **[insert position]** sending and receiving personal emails is permitted, provided that if emails are sent with **[insert organisation name]**'s address, a disclaimer is attached stating that the views of the sender may not represent those of the organisation.

[Sample Disclaimer - This email (and any file transmitted with it) is intended for the addressee only and may contain confidential information. If you have received this email in error, please delete it and notify the originator of the message. Any views expressed in this message are those of the individual sender except where the sender (with authority) states them to be the views of [insert organisation name]].

Emails related to the core business of **[insert organisation name]** will be stored **[insert location]** with back-up copies stored on the server and the **[insert position]** has access to them.

Email users will not compromise the privacy of their password by sharing it with others or exposing it to public view. Passwords will be changed on a regular basis.

Employees can generally expect that the subject and recipients of emails may be monitored intermittently.

[insert organisation name] reserves a right to read and take action on employee email if there is reasonable evidence that an employee is breaching the Guidelines for Use of Computer and Phones.

Email can be subject to production in litigation or other investigations.

Strictly Prohibited Use of Email

The use of **[insert organisation name]** email as follows is strictly prohibited:

- Reading or sending messages from another user's account, without **[insert organisation name]** authorisation

- Altering or copying a message or attachment belonging to another user without the permission of the creator of the message/attachment
- Subscribing to list servers and distribution lists unless they are directly related to your work or permitted by your supervisor
- Exchanging information in violation of copyright laws
- Exchanging proprietary information, trade secrets, or any other confidential or sensitive information about the company (unless in the authorised course of their duties)
- Creating or exchanging messages that are offensive, harassing, obscene or threatening
- Promoting web sites containing objectionable or criminal material
- Conducting a business or conducting illegal activities
- Creating or exchanging advertisements, solicitations, chain letters and other unsolicited or bulk email.

4.2 Internet Use

Employees, volunteers and students may use internet access provided by the organisation for any work-related purposes.

With permission from **[insert position]**, accessing the web is permitted for personal purposes, provided that personal use is moderate in time, does not incur significant cost to the company and does not interfere with the duties of the employee, volunteer, student or colleagues.

[insert organisation name] monitors logs of internet usage which may reveal information such as which servers (including websites) have been accessed by the employee and email addresses used.

The internet is used in a manner consistent with the Code of Conduct and as part of the normal execution of an employee's or volunteer's job responsibilities or student's learning needs.

Internet users will not compromise the privacy of their password by sharing it with others or exposing it to public view. Passwords will be changed on a regular basis.

Use of **[insert organisation name]** internet to undertake the following activities is strictly prohibited:

- Visiting web sites containing objectionable or criminal material
- Gambling, gaming, conducting a business or conducting illegal activities
- Installation of software without **[insert organisation name]** authorisation
- Creating or exchanging messages that are offensive, harassing, obscene or threatening

- Creating, storing or exchanging information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies)
- Exchanging proprietary information, trade secrets, or any other confidential or sensitive information about the company (unless in the authorised course of their duties).

4.3 Phone Use

Employees, volunteers and students may use phones provided by the organisation for any work-related purposes.

With permission from **[insert position]**, phone is permitted for personal purposes, provided that personal use is moderate in time, does not incur significant cost to the company and does not interfere with the duties of the employee, volunteer, student or colleagues.

Employees, students and volunteers will make all telephone calls as brief as possible.

Incoming Telephone calls

Employees, students and volunteers will answer the phone courteously and appropriately respond to callers' requests.

Outgoing Telephone Calls

[insert organisation name] employees, students and volunteers are able to make local telephone calls. **[insert position]** may authorise STD and international telephone calls.

When possible calls should be made to land lines instead of calling mobiles to minimise costs

Mobile Telephones

Employees, volunteers and students are responsible and accountable for the use, safe keeping and security of **[insert organisation name]** mobile phones issued on a loan basis to employees, volunteers and students and remain the property of the organisation.

Employees must abide by all Commonwealth and State laws when using a mobile phone.

Reference: *These guidelines are adapted from the NADA Guidelines for Use of Computers and Phones, AND Staff Email, Internet and Phone Use Guidelines.*

http://www.nada.org.au/index.php?option=com_content&task=view&id=236&Itemid=44