Curtin Information Technology Services (CITS) is responsible for ensuring Curtin University staff and students adhere to the Appropriate Use Guidelines.

All Information and data processed by, or stored on, Curtin University ICT facilities and services remains the property of the University. The University actively monitors the use of its ICT facilities and services, including the content of all electronic communications. A contravention of University ICT policies could result in disciplinary action.

**REPORTING A SECURITY INCIDENT**

All suspected Information Security incidents or activities involving inappropriate use must be reported by calling the CITS Service Desk on ext 9000 if you are a staff member or, by calling the Student Helpdesk on ext 1222 if you are a student.

**QUESTIONS**

Questions regarding the appropriate use of ICT facilities and services that are not outlined herein, should be directed to the Information Security team by email to info-security@curtin.edu.au or by calling ext 9750.

**DEFINITIONS**

“Staff” means the academic and non-academic staff of the University.

“Student” means a person enrolled in the University.

“University Associate” is a person who is neither a staff member nor principally a student of the University, but who has a continuing association with the University by virtue of their involvement in University activities.

**MALWARE**

Malware is malicious software used by attackers to disrupt computer operations, gather personal information, or gain access to a private computer. If your computer has been infected by malware, you will need to shut down your computer immediately. Notify the Information Security team by calling ext 9750.

**UNSOLICITED EMAILS (SPAM) AND PHISHING**

It is important that you do not respond to, or click on, any links in spam, phishing or suspicious emails, in particular emails that ask you to provide your username and password details, or any personal information.

Phishing emails often try to create a sense of urgency by stating such things as:

- ‘your account will be closed down unless you log on’
- ‘a recent security upgrade means that you have to log on to be protected’, or
- ‘there has been a problem with processing your payroll, you need to provide your account details to confirm that they are correct.’

If you receive a spam or phishing email please forward the email to spam@curtin.edu.au and promptly delete the email.

The above email address is used for reporting and statistical purposes only.

Curtin Information Technology Services (CITS) is responsible for ensuring Curtin University staff and students adhere to the Appropriate Use Guidelines.

All Information and data processed by, or stored on, Curtin University ICT facilities and services remains the property of the University. The University actively monitors the use of its ICT facilities and services, including the content of all electronic communications. A contravention of University ICT policies could result in disciplinary action.

**INFORMATION & COMMUNICATIONS TECHNOLOGY (ICT) APPROPRIATE USE GUIDELINES**

Curtin Information Technology Services (CITS) vision:

To be a high performing, flexible and responsive service organisation by developing our key capabilities and values in support of the rapidly changing needs of the University.

The ICT Appropriate Use Guidelines applies to everyone equally and defines appropriate and inappropriate behaviours when using Curtin’s ICT facilities and services.
INTRODUCTION

Curtin’s Policies and Procedures are binding on staff upon employment, upon students after enrolment, and upon any other person recognised as a University Associate.

If your association with Curtin falls into any of the above categories, it is your responsibility to become familiar with, and adhere to, Curtin’s Policies and Procedures, including those relating to ICT.

University information and ICT facilities and services are provided for the purpose of academic and University related business. When using University information and ICT facilities and services, users are responsible for ensuring that this is done in an appropriate manner, including University related activities which are performed on personal devices.

If you are uncertain about the information in this brochure, further detail can be found in the University Policies and Procedures. You can view Curtin’s ICT Policies and Procedures from any computer connected to the Internet, including computers in Curtin offices and student laboratories. These policies can be found at: http://policies.curtin.edu.au/.

APPROPRIATE USE GUIDELINES

The Appropriate Use of ICT Procedures applies equally to everyone using Curtin ICT facilities and services, including people using their own computers or portable electronic devices connected to the Curtin ICT network. Following are some examples of what is considered appropriate and inappropriate use of Curtin ICT facilities and resources.

DO

✓ Use only those ICT facilities and services for which you have authorisation.
✓ Use ICT facilities and services only for their intended purpose.
✓ Abide by applicable laws and University policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.
✓ Respect the privacy and personal rights of others.
✓ Use Curtin ICT facilities and services in a manner which is ethical, lawful and not to the detriment of others.
✓ Use Curtin ICT facilities and services for teaching, learning and academic purposes.
✓ Use ICT facilities for personal use where such use is incidental and does not impose upon or adversely affect the University, such as using ICT facilities and services for occasional emails and web browsing.

DON’T

✗ Access, copy, alter or destroy information, electronic mail, data, programs, or other files without authorisation.
✗ Use resources you have not been specifically authorised to use.
✗ Use someone else’s username and password or share your username and password with someone else.
✗ Upload, download, distribute or possess pornography, pirated software, movies, or other unlicensed digital media.
✗ Send unsolicited emails (spam).
✗ Use electronic resources for harassment or stalking.
✗ Possess any “hacking tools” such as packet sniffers, password crackers, vulnerability scanners without written authorisation from the Chief Information Officer (contact the Information Security team for assistance).
✗ Wilfully waste resources associated with Curtin’s ICT facilities and services.

EXEMPTIONS

Users may be granted an exemption to particular aspects of the Appropriate Use of ICT Procedures by the Chief Information Officer (CIO) where it can be clearly demonstrated that it is required for teaching, learning or research purposes. Users wishing to apply for an exemption should contact the Information Security team by emailing info-security@curtin.edu.au or calling ext 9750.