Acceptable Use of Technology Procedures

Table of Contents

1. Governing Policy

Information Security Policy

2. Purpose

A key principle in the Information Security Policy is that:

All users of digital information services are required to behave in a lawful, ethical, appropriate and responsible manner by:

a. employing all reasonable efforts to protect University-owned and personal computing devices that contain University information from physical theft, damage or unauthorised access

b. employing all reasonable efforts to protect the confidentiality of their user credentials and active login sessions

c. encrypting sensitive digital information assets prior to removal from the University network or campus, and

d. complying with the Supporting Procedures.

These procedures give effect to this principle by clarifying some of the specific responsibilities of all users of University technology.

3. Procedures

3.1. Accountability

Users are responsible for all activities originating from their University account (e.g. FAN, email address, student number, staff number).

University IT user	a. Do not share your FAN password with any other user. b. Report any suspected misuse of University IT resources to Information & Digital Services (IDS). c. Ensure sensitive information is only shared using secure methods of transmission. d. Take precautions to ensure that screens displaying sensitive or critical information are not seen by unauthorised persons in public areas and are locked when unattended.

Example: You are a staff member with access to the Student System. You sometimes work in the Student Hub and don't notice that a student is watching you type your password. When the student subsequently accesses your account, and makes unauthorised Student System changes, you are initially assumed responsible until proven otherwise.

3.2. Unlawful, unethical, inappropriate or irresponsible activities

University IT user	a. Comply with the terms and conditions of any licensed third-party software. b. Do not copy, download, store or transmit material that infringes copyright, including music files, movie/video files and/or software. c. Do not access any illegal or inappropriate online content or business activity. d. Do not create or transmit material/messages intended to offend, vilify, harass, discriminate and/or defame. e. Do not attempt to gain unauthorised access to any University systems or use University resources to gain unauthorised access to other systems. f. Do not attempt to subvert any security feature on University systems.

Examples: Using unlicensed Microsoft Visio; downloading "torrented" movies/music/games; viewing pornographic content; gambling online; using Flinders email address to login and comment negatively/abusively in online forums.

3.3. Monitoring of usage

University IT user	a. Be aware that all internet and digital information service usage activity is automatically recorded and monitored. b. Be aware that all electronic communications using University email/messaging systems: i. are recorded ii. are deemed official University correspondence iii. are subject to the Freedom of Information and State Records Acts, and iv. remain the property of the University.

3.4. Email usage

University IT user	a. Do not open any email attachment or hyperlink that is suspicious or from untrusted or unknown sources. b. Do not send junk email, for-profit messages, chain mail and/or unsolicited commercial emails.

3.5. Collaboration services

University IT user	a. Do not use collaboration tools for formal/official correspondence. Email and written correspondence are still preferred for such communication.

3.6. Telephone services

University IT user	a. Do not make calls to premium telephone numbers or international numbers unless approved beforehand by a College/Portfolio Head.

3.7. Personal use of University resources

University IT user	Use University IT Resources for personal use only if it does not: a. interfere with the performance of your job, studies or other University responsibilities b. interfere with normal IT operations c. interfere with the use or access of other users d. damage the reputation or operations of the University, and/or e. impose unreasonable additional costs on the University.

4. Supporting documentation

Freedom of Information Policy

Approval Authority	Vice-President (Corporate Services)
Responsible Officer	Chief Information Officer
Approval Date	21 December 2017
Effective Date	21 December 2017
Review Date*	December 2020
HPRM file number	CF18/17

* Unless otherwise indicated, this procedure will still apply beyond the review date.