

Acceptable Use of IT Resources Procedure

Section 1 - Purpose

- (1) The purpose of this Procedure is to set rules for and explain:
- a. Conditions of Use;
 - b. Access to Information Technology Resources;
 - c. Responsibilities of Authorised Users;
 - d. Misuse of IT Resources;
 - e. Liability; and
 - f. Monitoring and Surveillance of IT Resources.

Scope

- (2) This Procedure applies to Authorised Users of Macquarie University's Information Technology resources at all campuses and locations of the University.
- (3) To the maximum extent possible, this Procedure applies to all use of Information Technology Resources.

Section 2 - Policy

- (4) Refer to the [Acceptable Use of IT Resources Policy](#).

Section 3 - Procedures

Responsibilities and Required Actions

- (5) The following are the Responsibilities and Required Actions that underpin the [Acceptable Use of IT Resources Policy](#).

Conditions of Use

- (6) The University makes available its Information Technology Resources for the purposes of learning, teaching, research, administration and other University business.
- (7) It is a condition of access to the University's Information Technology Resources that Authorised Users accept:
- a. to comply with all the provisions of this Procedure;
 - b. agree to abide by any conditions of use applicable to the use of IT Resources as determined by the Chief Information Officer from time to time; and
 - c. that their actions and usage may be monitored and records retained.

- (8) The University plans to participate in eduroam:

- a. all users of eduroam facilities at participating organisations will be subject to the provisions of the policies of their home organisation, policies of the visited organisation, and the Australian eduroam Policy.
- b. participating organisations set their own access policies, which may be more restrictive than Macquarie University's [Acceptable Use of IT Resources Policy](#).

Access to Information Technology Resources

(9) General authorisation to use Information Technology resources is granted upon enrolment, employment, official affiliation with the University, or as a member of a participating eduroam organisation.

(10) Access to Information Technology Resources outside the purposes of learning, teaching, research, administration and other University business, except for limited personal use, is unauthorised. Unauthorised access to Information Technology Resources is a breach of the [Acceptable Use of IT Resources Policy](#).

(11) The Chief Information Officer or his or her delegate may impose such restrictions or conditions on the granting of authorisation to any person as he or she thinks fit, including:

- a. the mandatory use of a username and password, or other authentication method;
- b. restrictions or conditions as to the facilities the person is authorised to use; and
- c. the provision of acknowledgments by the person to the effect that he, she or it will abide by this Procedure and any applicable conditions of use, including:
 - i. written acknowledgments signed by the user; and
 - ii. requirements that the Authorised User click on or enter an acknowledgment as a condition of access to any IT Resources.

(12) Only Authorised Users are permitted access to University Information Technology Resources. System access to the Information Technology Resources is managed and granted by the Information Technology office.

(13) Access to some faculty-controlled or division-controlled Information Technology Resources is granted by authorised faculty or divisional staff. Access to specific resources may be further restricted depending on the University's requirements.

(14) Access to Information Technology Resources may be restricted or withdrawn if there is a reasonably formed suspicion or evidence of misuse of Information Technology Resources, a breach of any Macquarie University Rule, Regulation, Policy or the law.

Responsibilities of Authorised Users

(15) Each Authorised User is responsible for:

- a. usage of the unique computer accounts which the University has authorised for the user's benefit;
- b. selecting and keeping a secure password for each of these accounts, including not sharing passwords and logging off after using a computer;
- c. using the ICT facilities in an ethical and lawful way, in accordance with Australian laws and relevant local laws where a student is based in another country;
- d. ensuring that except for limited personal use, IT Resources are only used for authorised purposes;
- e. notifying the University Executive Information Policy Officer if they become aware that facilities are being used by any person to infringe the intellectual property rights of another person, or that the effect of any use of any facilities is to infringe such rights;
- f. co-operating with other users of the IT Resources to ensure fair and equitable access;
- g. observing the obligations under this Procedure;

- h. observing the Terms of Service or Acceptable Use policies of third party products or services that have been engaged by the University.

Misuse of IT Resources

(16) Misuse of Macquarie University's IT Resources is a breach of the [Acceptable Use of IT Resources Policy](#).

(17) Any member of the University community who becomes aware of possible misuse of Information Technology Resource must report it to either:

- a. their supervisor or manager;
- b. their Organisational Unit Head;
- c. the Director, Human Resources; or
- d. the Chief Information Officer.

(18) Misuse of IT Resources could result in revocation of access to IT Resources (see Access to Information Technology Resources).

(19) In the event of misuse, formal disciplinary action for students will occur in accordance the [Student Code of Conduct](#). Formal disciplinary action for staff will occur in accordance with the Misconduct / Serious Misconduct clauses as outlined in the Staff Code of Conduct, the [Macquarie University Academic Staff Enterprise Agreement 2018](#) and the [Macquarie University Professional Staff Enterprise Agreement 2018](#).

(20) Macquarie University may refer serious matters or repeated breaches to the Vice-President, People and Services, Director, Human Resources, the Head of the relevant Organisational Unit or to the appropriate external authorities which may result in civil or criminal proceedings.

(21) Macquarie University has a statutory obligation to report illegal activities and corrupt conduct to appropriate authorities and will cooperate fully with the relevant authorities.

Liability

(22) To the extent allowed by law, the University is not liable for loss, damage or consequential loss or damage arising directly or indirectly from

- a. use or misuse of any Information Technology Resources;
- b. loss of data or interference with data stored on any Information Technology Resources;
- c. interference with or damage to equipment used in conjunction with any Information Technology Resources;
- d. loss of data, access to IT Resources or interference with files arising from its efforts to maintain the IT Resources; or
- e. any acts taken or decisions made in accordance with this Procedure.

Monitoring and Surveillance of IT Resources

(23) The Chief Information Officer or their delegate may at any time monitor, inspect, access or examine any University IT Resources for any purpose permitted by the [Acceptable Use of IT Resources Policy](#), any other University policy, rule or regulations and for the purposes of:

- a. facilitating the efficient operation and management of the University IT Resources;
- b. protecting the integrity of IT Resources;
- c. investigating alleged misuse;
- d. auditing the assets of the University; or

- e. logging and Information Security.

(24) Specific provisions relating to Security Monitoring and Surveillance are outlined in [Information Security Procedure – Monitoring and Surveillance of IT Resources](#).

Section 4 - Guidelines

(25) Nil.

Section 5 - Definitions

(26) Commonly defined terms are located in the University Glossary. The following definitions apply for the purpose of this Procedure, unless a contrary intention appears:

- a. Authority means:
 - i. in relation to the IT Resources generally, the Chief Information Officer or the Chief Information Officer's delegate;
 - ii. in relation to a local facility, the relevant Head of Department, Executive Dean, or Deputy Vice-Chancellor, or a person nominated by the relevant head of department, Executive Dean, or Deputy Vice-Chancellor;
- b. authorised purposes means purposes associated with work or study in the University, provision of services to or by the University, which are approved or authorised by the relevant officer or employee of the University in accordance with University policies and procedures or pursuant to applicable contractual obligations, limited personal use, or any other purpose authorised by the relevant Authority;
- c. Chief Information Officer means the person holding or acting in that position in the University, or any other person nominated by the Vice-Chancellor to exercise that role for the purpose of this Procedure.
- d. Director, Human Resources means the person holding or acting in that position in the University, or any other person nominated by the Vice-Chancellor to exercise that role for the purpose of this Procedure;
- e. illegal material means material the creation, transmission, storage, downloading or possession of which contravenes or if done in New South Wales would contravene the law as it applies in any jurisdiction in Australia;
- f. Macquarie IT means the Macquarie University Information Technology office.
- g. intellectual property includes the rights relating to:
 - i. literary (including computer programs), artistic, musical and scientific works;
 - ii. multimedia subject matter;
 - iii. performances of performing artists, phonograms and broadcasts;
 - iv. inventions in all fields of human endeavour;
 - v. scientific discoveries;
 - vi. industrial designs;
 - vii. trademarks, service marks and commercial names and designations;
 - viii. plant varieties;
 - ix. circuit layouts; and
 - x. confidential information.
- h. limited personal use means use that:
 - i. is of a purely personal nature and not for financial gain;
 - ii. does not directly or indirectly impose an unreasonable burden on any IT Resources;

- iii. does not unreasonably deny any other user access to any facilities;
 - iv. does not compromise confidentiality or privacy obligations;
 - v. does not contravene any law in any jurisdiction in Australia or any University statute, regulation, policy or procedure; and
 - vi. in the case of staff, does not interfere with the execution of duties.
- i. misuse has the meaning set out in the [Acceptable Use of IT Resources - Misuse Schedule](#) to this Procedure;
 - j. staff means staff of the University;
 - k. student includes a person who was a student at the time of any alleged breach of this Procedure, and a person who is a student for the purposes of the [Student Discipline Rules](#) and [Student Discipline Procedure](#); and
 - l. Executive Information Policy Officer means the officer designated by the Vice-Chancellor as responsible for overseeing copyright issues within the University.

Status and Details

Status	Historic
Effective Date	22nd February 2021
Review Date	8th March 2021
Approval Authority	Vice-President, People and Services
Approval Date	10th June 2016
Expiry Date	28th April 2021
Responsible Executive	Eric Knight Deputy Vice-Chancellor (People and Operations)
Responsible Officer	Jonathan Covell Chief Information and Digital Officer
Enquiries Contact	Andrew Karvinen Chief Information Security Officer