Acceptable Use of IT Resources Policy

Section 1 - Purpose

(1) This Policy specifies requirements for the respectful, safe, reliable and secure use of Information Technology (IT) Resources provided by the University.

Background

(2) Information Technology Resources are vital for delivering the University's activities. The University is committed to maintaining a respectful, safe, reliable, and secure technology environment that allows the University to meet its organisational objectives, legal requirements, and ethical responsibilities.

Scope

(3) This Policy applies to:

a. all technology resources used by, operated by, or provided on behalf of the University (including its controlled entities);
b. all information collected, created, stored, or processed by, or for, the University on computer and network resources; and
c. all individuals who utilise, or are involved in deploying and supporting, computer and network resources provided by the University.

Section 2 - Policy

ACCEPTABLE USE

(4) All individuals who access, use or otherwise engage the University's IT Resources are required to:

a. respect the rights of all individuals, including other users;
b. only use or modify University IT Resources for Authorised Purposes, and not in breach of relevant laws or contractual obligations;
c. not use University computer or network equipment for non-commercial personal purposes beyond a reasonable amount, or to the detriment of the University or its goals;
d. not access, distribute, store or display illegal, pirated or offensive material;
e. not use University computer or network equipment for unauthorised personal financial or commercial gain;
f. not misrepresent the views of the University, via use of the University's IT Resources;
g. not conduct activities that consume excessive network bandwidth;
h. report suspected or actual security breaches to the Information Technology (IT) Service Desk in a timely manner; and
i. maintain the security and confidentiality of information generated or collected by the University in accordance with the Information Classification and Handling Procedure.

This document may be varied, withdrawn, or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Policy Central (https://policies.mq.edu.au) for the latest version.

SECURE SYSTEM ACCESS AND USE

(5) To protect access to University IT Resources, individuals are required to:

a. select long and strong passwords that are not easily guessed and not in use in other non-University applications;
b. not share University-provided or self-selected passwords with other individuals;
c. keep personal and University-provided systems, used to access University systems or information, free from known vulnerabilities by keeping up-to-date with vendor provided security updates;
d. maintain operational and up-to-date antivirus on personal and University-provided systems used to access University systems or information;
e. securely store passwords that provide access to University systems or information;
f. only use the accounts provided by the University for their own individual use;
g. not bypass or attempt to circumvent the University's Security Controls or Protection Mechanisms;
h. not introduce malicious software such as viruses, worms, ransomware or trojans into the University environment; and
i. not use Hacking Tools (including sniffing, scanning, password guessing or exploitation) when accessing, using or otherwise engaging with University IT Resources.

MONITORING AND COMPLIANCE

(6) The University monitors its information systems for compliance with this Policy in accordance with the University's Workplace Surveillance Policy. Breaches of this Policy constitute misuse of University's information and information systems.

(7) The Acceptable Use of IT Resources - Misuse Schedule provides some examples of activities that constitute misuse of IT Resources. If misuse of IT Resources is detected or suspected, relevant disciplinary provisions will be invoked.

(8) The University may refer serious matters or repeated breaches to the Chief Information and Digital Officer, Chief People Officer, the Head of the relevant organisational unit, or the appropriate external authorities which may result in disciplinary and/or civil, and/or criminal proceedings.

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

(10) To the extent allowed by law, the University is not liable for loss, damage or consequential loss or damage arising directly or indirectly from the use or misuse of any Information Technology Resources.

Section 3 - Procedures

(11) Nil.

Section 4 - Guidelines

(12) Nil.

Section 5 - Definitions

(13) The following definitions apply for the purpose of this Policy:

a. Authorised Purposes means activities associated with work or study at the University, or 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 officer or employee.
b. Hacking Tools means tools that are designed to facilitate the identification and exploitation of software or system weaknesses for the purposes of unauthorised access.
c. Information Technology Resources, or IT Resources, includes, but is not limited to:
    i. All computers and all associated data networks and systems, internet access and network bandwidth, email, hardware, data storage, computer accounts, all OneID systems, media, software (both proprietary and those developed by the University) and telephony services.
    ii. Information Technology services provided jointly, or as part of a joint venture between the University and a research centre, school, institute affiliated with the University, a subsidiary organisation owned by the University or any other partner organisation.
    iii. Information Technology services provided by third parties that have been engaged by the University.
d. Security Controls or Protection Mechanisms means systems or facilities implemented to restrict access only to individuals who are authorised to access or utilise the resource or information.

This document may be varied, withdrawn, or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Policy Central (https://policies.mq.edu.au) for the latest version.

Status and Details

Status	Current
Effective Date	29th July 2024
Review Date	29th July 2027
Approval Authority	Vice-President, Professional Services
Approval Date	28th July 2024
Expiry Date	Not Applicable
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

This document may be varied, withdrawn, or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Policy Central (https://policies.mq.edu.au) for the latest version.