Acceptable Use of RMIT Network, Internet and Email Standard

What is it?

This document outlines minimum behaviours for all users of RMIT information technology assets. It aims to protect information, individuals, and our operations from harm and misuse, and illustrates typical IT-related activities that are considered acceptable and unacceptable.

The Standard is a resource to the RMIT Information Technology and Security Policy, that sets out the minimum behaviours to ensure all access and use of RMIT information and information systems is appropriate.

This Standard has been aligned to AS ISO/IEC 27002:2015, Information technology - Security techniques - Code of practice for information security controls.

Who is this for?

This Standard applies to all individuals who have access to RMIT's information or information systems including RMIT Group staff, students, casual employees, contractors, visitors, third parties (suppliers), and agents of the organisation who are bound to RMIT policy where their contract of engagement with the University specifically provides for this.

1. Standard requirements

1.1. Acceptable use of technology and University provided internet

Standard	Description
AU-010	Access and use IT systems and facilities must be for legitimate university work purposes
AU-020	Access and use IT facilities for personal or recreational purposes, provided; • such use is reasonable • does not adversely affect other IT users • is entirely legal Such use is a privilege, not a right, and may be withdrawn at any time
AU-030	Activities unacceptable within this Standard must be explicitly authorised by a policy exemption endorsed by the Chief Information Security Officer (e.g. penetration testing by specific individuals, issuance of passwords to users by Security Administration)

1.2. Unacceptable use of IT includes the following:

Standard	Description
AU-050	Creating, using, saving or distributing material that might reasonably be considered offensive, obscene or indecent by an ordinary member of the public (e.g. pornographic or racist matter)
AU-060	Plagiarising, copying or distributing information in contravention of copyright and similar legal obligations (i.e. “piracy”)
AU-070	Using IT systems to annoy, inconvenience, harass or defame others, including the distribution of spam, malicious rumours and so forth
AU-080	Sharing or disclosing personal user identities, passwords, security tokens etc. with anyone else
AU-100	Hacking or probing for security vulnerabilities in networks, systems etc.
AU-110	Deliberately creating, introducing or distributing computer viruses or other malicious software
AU-120	Stealing, disclosing or disposing of information assets including proprietary and personal data, IT hardware etc. without proper authority
AU-130	Connecting IT devices to the University network or systems deemed by the CISO to be unsecure
AU-140	Monitoring, intercepting or otherwise accessing network traffic, emails, files etc. intended for another person
AU-150	Using company IT facilities for work for another organisation, even not-for-profits
AU-160	Excessive use of IT storage or processing capacity that impacts other users

1.3. Acceptable use of RMIT internet access

Standard	Description
AU-260	Accessing information from the Internet and using general Internet services (such as email) for legitimate work purposes
AU-270	Accessing and using the Internet for personal or recreational purposes, provided such use is incidental and reasonable, does not conflict with other network or Internet use, and does not constitute unacceptable use
AU-280	Activities on the “unacceptable use” list if they have been explicitly pre-authorised (in writing) by management for legitimate business reasons

1.4. Unacceptable use of RMIT internet access

Standard	Description
AU-340	Up/downloading or distributing illegal material or visiting websites which might be considered offensive, obscene or indecent by an ordinary member of the public (e.g. pornographic or racist)
AU-350	Making additional Internet connections, even temporarily, without having been pre-authorised by management and/or without applying appropriate IT security controls

AU-360	Storing corporate or personal information on Internet-based backup or file server sites without strong encryption
AU-370	Downloading or running software other than JavaScript and similar utilities required to interact with websites and web services
AU-380	Commercial or charitable activities not expressly sanctioned by management
AU-400	Entering into contractual relationships or making other legally-binding commitments on behalf of the organisation
AU-410	Appearing to represent the University or it's entities without due authorisation
AU-420	Disclosing confidential (personal or proprietary) information through websites, blogs, discussion forums etc.
AU-430	Annoying, inconveniencing, harassing or defaming others (e.g. distributing spam, insults or malicious rumours)
AU-440	Hacking, attempting to break-in or probing web sites for security vulnerabilities etc.
AU-450	Up/downloading or distributing unauthorised malware, hacking tools etc.
AU-460	Intellectual property theft (e.g. using copyright images, text, videos or sounds from websites without the owners' express permission)
AU-470	Unnecessarily consuming Internet bandwidth (e.g. up/downloading large non-work-related video files in peak work hours)

1.5. Email use

Standard	Description
AU-480	Staff must not set up auto forwarding of RMIT email to personal email accounts
AU-490	Upon staff departure from RMIT, emails remain the property of RMIT and may be retained or deleted at the discretion of the CISO. CISO must give consideration to data retention obligations
AU-500	Former staff returning to RMIT may get access to their past emails if they return to their former role (or by policy exemption approved by RMIT CISO)
AU-520	RMIT must train staff in the detection and reporting of suspicious email. This may include the regular and frequent sending of simulated phishing emails and targeted training to staff
AU-530	Emails must be classified using sensitivity settings in Outlook based on the sensitivity of information contained in content, links and attachments
AU-540	User email accounts must not share a password
AU-550	Use of shared (group) email boxes must be configured so an email sender is not anonymous and at least two people share ownership

2. Information security standards exemptions

2.1. Exemptions from the information security standards and other RMIT policies relating to ITS use, must be sought using the ITS policy exemption request process determined by the Chief Information Security Officer.

2.2. Exemptions must be sought prior to undertaking investigation of alternatives.

3. Compliance

3.1. Repeated non-compliance with this Standard may result in disciplinary action, including legal action. Management will decide what action to take, if any, based on the severity of the incident(s).

3.2. All staff are collectively and individually accountable for minimising information security risks, ensuring data privacy, and avoiding avoidable information security incidents.

More information

These are not exhaustive lists. Speak to your manager, HR, the Help Desk or the Information Security Manager if:

- you are uncertain whether other activities are acceptable or not; or
- you are uncertain about whether a standard applies to a given situation.

Browse the Security Zone for general advice including other policies.

Document history

Version	Effective date	Authority	Author	Register reference
1.0	2 March 2020	Information Technology and Security Policy	Chief Information & Security Officer	POL/2020/00009