Information Technology - Acceptable Use Standard

Section 1 - Purpose

(1) The objective of this Standard is to:

a. provide guidance and define enforceable standards for using RMIT information technology (IT) assets
b. protect RMIT IT assets and provide a reliable information technology infrastructure, and
c. protect and maintain RMIT reputation.

Section 2 - Scope

(2) This standard applies to all students, staff, contractors, visitors and any other parties who have access to the IT assets of RMIT University and its controlled entities ('RMIT').

Section 3 - Authority

(3) Authority for this document is established by the Information Technology and Security Policy.

Section 4 - Standard

Principles

(4) Access and use of IT assets must be for legitimate RMIT purposes, specific to the user's role, and in accordance with RMIT policies, procedures and standards.

(5) Access and use of IT assets for reasonable non-commercial personal purpose is acceptable, provided such use:

a. does not directly or indirectly impose an unreasonable burden on any RMIT IT assets
b. does not burden RMIT with incremental costs
c. does not interfere with RMIT staff executing their responsibilities.

(6) Access and use of RMIT IT assets for any commercial purpose other than legitimate RMIT purposes is not allowed.

(7) Any use of RMIT IT assets is not acceptable when it is used for any act which:

a. is not legal
b. negatively impacts RMIT's reputation
c. adversely impacts continued operation of RMIT
d. adversely affects other RMIT IT users, or
e. is a breach of RMIT policies, procedures and standards including, but not limited to, Code of Conduct, Workplace

Behaviour Policy, Student Charter, Student Conduct Policy, Delegations of Authority Policy, Intellectual Property Policy, and Information Technology - User Device Security Standard.

A list of examples of unacceptable IT usage is given in Appendix A: Examples of Unacceptable Use - RMIT IT Assets.

(8) Speak to your manager, College or Portfolio management, People team, or the Information Technology Services (ITS) Service and Support Centre if you are uncertain whether other activities are acceptable or not, or you are uncertain about whether a standard applies to a given situation.

User Behaviour

(9) To protect RMIT Information everywhere, users must:

a. ensure all non-public printed or digital information is kept discrete and secure
b. not allow student or staff personal information to be included when taking photos or videos in RMIT office environments
c. screen lock devices when not in use
d. not take RMIT IT asset offsite (other than laptops/mobiles, which are specifically assigned to them and expected to be mobile) without prior authorisation from ITS or relevant College or Portfolio manager.

(10) Users must only access, use and share RMIT information on a need-to-know basis. They must:

a. ensure they are authorised to share protected or restricted information
b. ensure the recipient is authorised to receive RMIT information
c. share only the minimum information required for the task.

(11) Users must dispose RMIT IT assets in a secured manner and in accordance with the Retention and Disposal Standard. This includes:

a. using secure waste when disposing of non-public hard copy information
b. returning to ITS all RMIT devices due for disposal.

(12) Information security is a shared responsibility. All users must play their role in keeping RMIT safe by:

a. changing their password immediately and reporting to the ITS Service and Support Centre if they suspect their RMIT password is compromised
b. not writing down RMIT password or leaving them in a place where an unauthorised person might discover them
c. not using RMIT password or PIN for non-RMIT applications or services
d. not sharing password or multi-factor authentication code or one time password (OTP) with anyone
e. classifying RMIT emails and documents based on sensitivity of the information
f. reporting any event that may put RMIT IT assets at risk of compromise or unauthorised disclosure, whether accidental or intentional, to:
    i. their manager, Portfolio or College management, and
    ii. ITS Service and Support Centre
g. reporting phishing emails using Microsoft Outlook’s phishing report feature.

Monitoring

(13) RMIT conducts surveillance across all systems and devices to determine any security weakness or policy non-

compliance.

(14) Use of RMIT IT assets is a privilege, not a right. RMIT has full rights to withdraw access to RMIT IT assets at any time without prior notification.

(15) RMIT may block any email or communication, inbound or outbound, that threatens the security of RMIT IT assets.

Information Security Standard Exemptions

(16) Exemptions from the Information Technology and Security Policy and related standards must be sought using the ITS Policy exemption process determined by the Chief Information Security Officer.

Compliance

(17) Non-compliance with this standard may result in a disciplinary action, or legal action in cases of illegal activity. Management will decide what action to take, if any, based on the severity of the incident.

Appendix A - Unacceptable IT Use Examples

(18) Creating, using, saving, accessing or distributing material is prohibited if it might reasonably be considered offensive, obscene or indecent by an ordinary member of the public, or is illegal (e.g. pornographic, racist or sexist material, or violent content), except where such items are legitimately held within the RMIT curated collections such as Art, Archival or Library Collections. Accessing or distributing material for legitimate research or educational purposes must have been granted an exemption through the ITS Policy Exemption Form.

(19) Plagiarising, copying or distributing information in contravention of copyright or similar legal obligations without the owners' express permission (e.g., copyright images, text messages, videos, memes or sounds from websites owned by a third party).

(20) Using IT systems to harass, bully or defame (e.g. spreading of malicious information via email).

(21) Unauthorised attempts to interfere with the operation of or make RMIT IT systems or services unavailable (e.g. flooding a booking system with fake bookings).

(22) Sharing or disclosure of personal user identities, identifiers and passwords, or security codes.

(23) Writing down passwords or leaving them in a place where an unauthorised person might see them.

(24) Unauthorised hacking or probing for security vulnerabilities in networks, systems or applications etc. without the written consent by the Chief Information Security Officer (CISO) (e.g. students or staff probing Canvas for vulnerabilities to exploit).

(25) Creating, introducing, or distributing computer viruses or other malicious software onto any RMIT network device or system.

(26) Disclosing, removing, or disposing of IT assets without authority from ITS, College or portfolio executive management. Such authority must comply with all RMIT policies, including the Information Governance Policy (e.g. taking a monitor home or using a staff contact database without permission, destruction of RMIT records within the mandated legal period).

(27) Monitoring, intercepting, or accessing network traffic, emails, files, etc. intended for another person.

(28) Deliberate unauthorised access to systems or data and/or unauthorised use of data or information obtained

(e.g. using someone’s unlocked computer to act on their behalf).

(29) Storing non-public information on non-RMIT endorsed site or location such as a USB drive, cloud storage or forwarding RMIT email to your personal email account (e.g., saving a student class listing on a personal storage service such as personal Dropbox or Box etc.).

(30) Transmitting unsolicited commercial advertising material or any other form of unsolicited commercial electronic message, including material commonly known as spam, or junk email (e.g., perpetuating chain letters, virus warnings or hoax messages).

(31) Responding to spam or phishing messages by supplying non-public RMIT or personal information.

(32) Using non-RMIT supplied VPN services or anonymisation technologies like VPN and TOR to access RMIT network, applications or services is not permitted (e.g. MobileVPN, ExpressVPN, etc.)

(33) Using applications on RMIT computers that allow for remote control of those computers from other locations. (e.g. TeamViewer, AnyDesk, etc.)

(34) Auto forwarding of RMIT email to non-RMIT managed devices or personal email accounts.

(35) Downloading, installing or running software, applications or software as a service (SaaS) that are not endorsed by ITS (e.g. Bitcoin miner, SpeedUpMyPC, etc.).

(36) Copying or distributing to unauthorised users software developed by, procured by or licensed to RMIT including computer software and cloud services.

Status and Details

Status	Current
Effective Date	3rd June 2024
Review Date	3rd June 2029
Approval Authority	Senior Policy Advisor
Approval Date	18th April 2024
Expiry Date	Not Applicable
Policy Owner	Fiona Notley Chief Operating Officer
Policy Author	Sinan Erbay Chief Information Officer
Enquiries Contact	ITS Governance, Risk and Compliance