Information Governance Policy

Section 1 - Purpose

(1) This policy establishes the framework and principles for effective data and information (Information) governance which supports the functions and activities of the RMIT Group.

Section 2 - Overview

(2) RMIT is committed to managing Information as an organisational asset that is created, used and shared effectively while meeting legislative requirements.

(3) Information governance provides the framework, strategic objectives, policies and standards to manage Information as an asset. This policy, supporting procedures and associated resources support effective Information governance to optimise the integrity, security, availability and quality of RMIT Information.

Section 3 - Scope

(4) Throughout this policy, RMIT means the RMIT Group. The RMIT Group is defined as RMIT University and its controlled entities (e.g. RMIT Vietnam, RMIT Europe, RMIT Online and RMIT University Pathways (RMIT UP)).

(5) This policy applies to all individuals who manage, handle or process RMIT Group Information, including RMIT Group staff, students, casual employees, contractors, visitors and honorary appointees. This also includes 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.

(6) This policy excludes research data as defined by the Research Policy

(7) This policy applies to the creation, storage, management, control, access, transfer and destruction of Information throughout its lifecycle in all its forms: both in digital and non-electronic formats.

Section 4 - Policy

Principles

(8) Data Quality from creation - RMIT implements procedures and practices to ensure that Information is captured accurately and completely, and that the quality of Information is monitored, managed and continuously improved throughout its lifecycle.

(9) Information is discoverable - RMIT Information classification is applied to enable appropriate management of Information, to ensure Information is easy to find and to promote its re-use.

(10) RMIT supports openness and collaboration - RMIT Information is accessible and transparent. Access to Information should only be restricted when required by legislation, policy or contract.

This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as unauthorised and should not be relied upon as the current version. It is the responsibility of the reader to refer to RMIT's Policy Register for the latest version of this document.

(11) Information is protected from unauthorised access, use and disclosure - RMIT Information is managed in accordance with procedures and resources established by this policy, the Privacy Policy, and the Information Technology and Security Policy.

(12) Information is retained, managed and disposed of lawfully and ethically – RMIT Information collection, creation, use, re-use and exchange is performed according to ethical practices, applicable laws and with due consideration for individual privacy.

(13) RMIT is a digital organisation - Information is created and retained in a digital format unless otherwise required by legislation.

(14) A data-literate workforce - RMIT is committed to ensuring that staff have the knowledge, competencies and ability to interact with Information in their roles. RMIT provides staff development through a Data Literacy Program and access to training materials.

Information Governance Framework

(15) Information Governance is established based on Information Domains, as defined in the RMIT Data and AI Catalogue.

(16) The Information Governance Board (IGB) provides advice and recommendations for strategy, policy and risk-related matters impacting RMIT's Information.

(17) Information Governance priorities are guided by the value of Information to RMIT, government and the community over time, considering the risks of improper management of Information.

(18) RMIT is the custodian of all Information managed by RMIT. No individual function or group own any part of Information.

(19) An individual assumes the role of Information Custodian when RMIT Information is in their possession.

(20) Information Governance controls are defined in consultation with Information Stewards. The Information Stewards Group (ISG) is established to provide operational support and recommendations to the Information Governance Board.

Responsibilities

(21) All individuals who manage, handle or process RMIT Group Information as set out in the scope of this policy are responsible for:

a. ensuring that they understand and adhere to the framework and principles established by this policy
b. managing RMIT's Information in accordance with procedures and resources under this policy, the Privacy Policy and Information Technology and Security Policy
c. supporting a culture that promotes good Information governance practices and reporting any identified compliance breaches or incidents.

(22) Information Custodians are:

a. responsible for ensuring that appropriate controls and processes are in place for the protection of Information under their custodianship in accordance with all applicable policies, legislation and contractual agreements
b. accountable for decisions and implications of access to Information under their custodianship. This includes Information sharing and access, movement of Information, physical protection and integration between systems.

(23) The Information Governance Board (IGB) and its members are responsible for:

a. providing strategic direction and advocating for Information governance in the best interests of RMIT.

(24) Information Trustees are:

a. accountable for Information governance decisions that impact how Information is managed in their Information Domain
b. responsible for nominating Information Stewards for their Information Domain.

(25) Information Stewards are responsible for:

a. providing operational support to Information Trustees and relevant stakeholders for Information within their respective domains as set out in the RMIT Data and AI Catalogue
b. taking steps to improve the quality and compliance of Information identified as high-priority to RMIT in the RMIT Data and AI Catalogue.

(26) The Chief Data and Analytics Officer is responsible for:

a. overseeing Information governance at RMIT to ensure effectiveness and fitness for purpose
b. establishing an Information Governance Network comprised of Information Stewards and Information Trustees
c. promoting a data-driven culture and encouraging RMIT staff to develop capability, competency and knowledge to interact with Information in their roles.

(27) The Chief Information Officer is responsible for:

a. providing Information Technology services for storage, processing, safekeeping and the integrity of Information in digital formats under the custodianship of RMIT
b. implementing appropriate safeguards without creating unjustified obstacles to the conduct of RMIT operations and the provision of services, as specified in the Information Technology and Security Policy.

(28) The Chief Information Security Officer is responsible for:

a. implementing appropriate Information and Information security controls, processes and technologies to protect RMIT from cybersecurity threats
b. monitoring and improving the effectiveness of security controls for Information in digital formats under the custodianship of RMIT.

(29) The Privacy Office is the first point of contact for privacy matters within RMIT and is responsible for:

a. overseeing responsible handling of personal, sensitive and health information in all its forms, consistent with relevant legislation, as specified in the RMIT Privacy Policy.

Compliance

(30) Investigations of breaches of this policy or non-compliance with legislation are undertaken in accordance with the Compliance Breach Management Procedure.

(31) This policy, as well as procedures and resources under this policy, include consideration of compliance requirements from the following legislation:

a. Crimes Act 1958 (Vic)

b. Data Availability and Transparency Act 2022 (Cth)
c. Freedom of Information Act 1982 (Vic)
d. General Data Protection Regulation (EU)
e. Health Records Act 2001 (Vic)
f. National Vocational Education and Training Regulator Act 2011
g. Privacy Act 1988 (Cth)
h. Privacy and Data Protection Act 2014 (Vic)
i. Public Records Act 1973 (Vic)
j. Tertiary Education Quality and Standards Agency Act 2011 (Cth)
k. Vietnam's Decree 53/2022/ND-CP (Vn).

(32) This policy is to be read in conjunction with existing University policy documents which include but are not limited to the following:

a. Research Policy
b. Privacy Policy
c. Information Technology and Security Policy
d. Intellectual Property Policy.

Review

(33) The Information Governance Board will review this policy annually and undertake a major review every five years in accordance with the Policy Governance Policy.

Section 5 - Schedules

(34) This policy includes the following schedule(s):

a. Information Classification Levels Schedule 1.

Section 6 - Procedures and Resources

(35) Refer to the following documents, which are established in accordance with this policy:

a. Classification of Analytics Data Standard
b. Data and Information Lifecycle Management Procedure
c. Data Quality Guideline
d. Data Quality Standard
e. Destruction of Information Procedure
f. Information Classification and Handling Procedure
g. Information Classification Standard
h. Key Term Definition Standard
i. Master Data Management Standard
j. Responsible Artificial Intelligence (AI) Procedure
k. Retention and Disposal Standard
l. Source Data Extract Controls Standard

This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as unauthorised and should not be relied upon as the current version. It is the responsibility of the reader to refer to RMIT's Policy Register for the latest version of this document.

(36) Local resources are available via the Data and Analytics website.

Status and Details

Status	Current
Effective Date	14th March 2023
Review Date	14th March 2028
Approval Authority	Senior Policy Advisor
Approval Date	9th March 2023
Expiry Date	Not Applicable
Policy Owner	Fiona Notley Chief Operating Officer
Policy Author	Nicola Burgess Interim Executive Director, Technology
Enquiries Contact	Data Management and Governance +61 3 9925 8000

This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as unauthorised and should not be relied upon as the current version. It is the responsibility of the reader to refer to RMIT's Policy Register for the latest version of this document.