Information Governance Policy

Section 1 - Purpose

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

Section 2 - Overview

(2) RMIT University is a public institution under Victorian law and stands on Aboriginal Country of the Kulin Nation. RMIT recognises and acknowledges the Bundjil Statement that helps all RMIT staff to respectfully work, live and study on Aboriginal Country.

(3) RMIT is committed to managing information as an organisational asset which is created, used and shared effectively whilst meeting legislative requirements.

(4) Information governance provides the framework, strategic objectives, policies and standards to manage information as an asset. This policy and supporting procedures and resources support the strategic plan of the organisation to drive outcomes and support continuous improvement and ultimately optimise integrity, security, availability and quality of information.

Section 3 - Scope

(5) This policy applies to all RMIT staff including staff of controlled entities, students, temporary employees, contractors, visitors and third parties globally who manage RMIT information with the exception of research data as defined by the Research Policy.

Section 4 - Policy

Principles

(6) RMIT is the custodian of all information managed by the RMIT Group. No individual function or group own any part of data or information.

(7) RMIT will take reasonable and necessary steps to ensure information security protection. Information Security Classifications will enable appropriate management of information.

(8) RMIT information will be

a. collected, created, managed, used, re-used and shared according to ethical practices, any applicable laws and with due consideration to individual privacy.
b. appropriately stored to ensure protection from loss and unauthorised access.
c. accessible, transparent and available to be used and shared whilst respecting matters of identity, privacy and confidentiality. This applies to internal as well as third party data.

d. managed in accordance with records management and archiving requirements.

(9) RMIT will implement procedures and practices to ensure all information is captured accurately and completely and managed throughout its lifecycle.

(10) RMIT will provide access to formal or informal learning material to ensure staff have the knowledge, competencies and ability to interact with information in their roles.

Responsibilities

(11) Information governance is overseen by the Chief Data and Analytics Officer (CDAO) with sponsorship of the Vice-Chancellor's Executive (VCE).

(12) The Information Governance Board provides an information governance forum for the RMIT Group.

(13) The Information Trustees are accountable for their respective domain area as set out in the Information Domain Register.

(14) The Information Stewards Group (ISG) provide operational support and recommendations to the Information Governance Board.

(15) The Information Stewards are responsible for identifying and managing information-related risks and issues for their assigned information entities and for escalating these to the data trustees accordingly.

(16) All RMIT staff including staff of controlled entities, students, temporary employees, contractors, visitors and third parties are responsible for:

a. ensuring the quality and completeness of information which they collect or create
b. ensuring that they understand and adhere to procedures and resources under this policy which govern the management, control, storage, transfer and destruction of information throughout its lifecycle
c. supporting a culture that promotes good information governance practices and reporting any identified compliance breaches or incidents
d. managing RMIT information in accordance with the Privacy Policy and Information Technology and Security Policy.

Compliance

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

(18) 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

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

Section 5 - Schedules

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

a. Schedule 1 – Security Classification Levels

Section 6 - Procedures and Resources

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

a. Classification of Analytics Data Standard
b. Destruction of Information Procedure
c. Information Management Standard
d. Key Term Definition Standard
e. Long Term Storage of Information Standard
f. Master Data Management Standard
g. Retention and Disposal Authority Standard
h. Source Data Extract Controls Standard

(22) Local resources are available via the Data & Analytics website.

Section 7 - Definitions

Data	Data is a fundamental component of information. It forms the building blocks of information. Data includes metadata, reference data and derived data. The definition of data in this policy excludes 'Research Data' as defined and governed by the Research Policy.
Information	Information is data in context which has relevance and is timely. For the purpose of this policy, the term 'information' refers to information, records and data, with the exception of 'Research Data' as defined and governed by the Research Policy.
Record	Information in any format created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. Records include (but are not limited to) emails, documents, websites, photographs, conversations undertaken via Instant Messaging clients, meeting minutes, research data, posts to RMIT social media sites.
Chief Data and Analytics Officer (CDAO)	The Chief Data and Analytics Officer is appointed to provide organisation-wide oversight of all data and information related functions. This includes providing strategic guidance for data governance across the whole organisation including information management, records management, data quality management, analytics, business intelligence, data security and data privacy.
Information Governance Board (IGB)	The IGB recognises information as a valuable asset and advocates for information governance. The IGB endorses strategy, provides strategic advice for information governance activities and issues, monitors progress against strategy, ensure risks are managed and that decisions are made in accordance with all applicable policies and regulations. Further details are set out in the Information Governance Board Terms of Reference.
Information Trustee	An information trustee is accountable for one or more domains of RMIT's information. This accountability is outlined in the Information Domain Register. The information trustee may delegate the management and handling of operational responsibilities associated with the information asset to an information steward.

Information Stewards Group (ISG)	The ISG is comprised of Information Stewards who provide operational oversight of information governance activities, identify information governance issues, identify opportunities for improvement, provide support for resolving issues and harnessing opportunities and escalating these to the IGB where appropriate for comments, decisions, approval or sponsorship. Further details are set out in the Information Stewards Group Terms of Reference.
Information Steward	An information steward is responsible for ensuring that information assigned to them by the information trustee is meeting RMIT's requirements. This includes monitoring, managing and escalating any risks and issues associated with the information.

Status and Details

Status	Historic
Effective Date	19th October 2020
Review Date	3rd September 2022
Approval Authority	Audit and Risk Management Committee
Approval Date	1st September 2020
Expiry Date	13th March 2023
Policy Owner	Clare Lezaja Chief Financial Officer
Policy Author	Nonna Milmeister Chief Data and Analytics Officer
Enquiries Contact	Data and Analytics

Glossary Terms and Definitions

"RMIT Group" - The University, its controlled entities and strategic investment vehicles (known as the RMIT Group).

"Record" - Information in any format created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. Records include (but are not limited to) emails, documents, websites, photographs, conversations undertaken via Instant Messaging clients, meeting minutes, research data, posts to RMIT social media sites.