Information Management Standard

Section 1 - Purpose

(1) This standard foregrounds RMIT's commitment to information management and its approach to the compliant handling of information in digital form, in compliance with relevant legislation.

Section 2 - Authority

(2) Authority for this document is established by the Information Governance Policy.

Section 3 - Scope

(3) This standard applies globally to any person or entity of the RMIT Group, including staff, students, temporary employees, contractors, visitors and third parties who manage RMIT information; with the exception of research data as defined by the Research Policy.

Section 4 - Standard

Overview

(4) RMIT must comply with standards issued under the Public Records Act 1973 (Vic) by the Public Record Office Victoria (PROV). These standards specify how the information we create as part of our work – or records - must be managed.

(5) The Information Governance Policy establishes a framework for effective information governance. This standard supports the policy by providing clear information management requirements for information in digital form that underpin the embedding of information management into day-to-day practices by default, so that information is complete, authentic and reliable evidence of RMIT's actions and decision making.

(6) These requirements apply to information, also known as unstructured data, wherever it is received, created or managed including (but not limited to) email systems, productivity tools, business or applications in digital form. This compliance by design approach enables RMIT to build compliance into its systems and processes so that we can:

a. gain visibility over current risks
b. mitigate risks where possible
c. accept residual risks where necessary .

Application Guidance

(7) These requirements should be implemented using a risk and value-based approach. Measures taken to ensure compliance should be reasonable and commensurate with the risk presented by the information; they should be followed more closely for high-value information or information needed to mitigate high business risk.

(8) Indicators of high-value business information include that it:

a. is critical to business continuity and/or accountability
b. affects the rights and entitlements of students, staff, or the broader community
c. significantly affects workplace health and safety
d. is subject to a high level of scrutiny (i.e., audits and freedom of information requests) or has a high likelihood for legal action
e. involves large sums of funding.

Requirements

(9) Information is created and managed digitally throughout its life.

a. Information should be created and managed in hardcopy only by exception. Exceptions may include where a document must be created and maintained in hardcopy for legal reasons.
b. Information must be maintained in a format that is expected to survive and be readable for the required life of the information, as defined in the Retention and Disposal Authority Standard (RDA Standard).

(10) Information must be retained according to legal and business requirements and disposed of lawfully when their retention period ends.

a. Information must be retained in accordance with the RDA Standard for as long as required.
b. Information must be disposed of – either destroyed/deleted or transferred – in accordance with the Destruction of Information Procedure.

(11) Information is to be shared. Access to information held by RMIT must not be restricted, unless required by legislation or in accordance with policy or authorised criteria.

a. RMIT must support openness and transparency by only restricting access to information when required by legislation, regulation or policy. These may include freedom of information exemptions or privacy principles for personal information.
b. Unauthorised access and unlawful deletion must be prevented.

(12) Controls must be designed and implemented to ensure information is only accessed, amended, used, released, or disposed of as authorised.

a. Evidence of the integrity, authenticity and reliability of information must be captured and retained for its lifetime.
b. This may be demonstrated by capturing appropriate audit trails and version control (i.e. who performed which action on what information at what time, major amendments must be documented).
c. Business continuity and disaster recovery planning must ensure information can be retrieved in the event of disaster.

(13) Information must have sufficient description to allow access and management over time.

a. The minimum will include the following metadata elements: title, creator, date created, and a unique identifier.

(14) Information must be managed to facilitate migration or relocation over time to ensure required retention.

a. This may include managing information and data beyond the life of the system (e.g., the reasonable

likelihood of the need for migration to systems must be assessed) .

b. Considerations should include (but not be limited to) the export capabilities of tools and applications used, the formats in which information can be extracted and the ability to extract information in a timely manner – either by RMIT or vendor.

Responsibilities

(15) Managing information compliantly is everyone's responsibility and all staff, students, researchers and affiliates have an obligation to manage the information they receive, create, collect, manage, use or re-use during their engagement with RMIT in accordance with this standard, the Information Governance Policy and relevant information security, information privacy and data governance policies.

(16) Managers are required to ensure that information management principles and practices are implemented locally, and suspected or actual breaches of this standard are reported in accordance with the Compliance Breach Management Procedure.

(17) Information Trustees as owners of information must review any risks to information within their remit caused by non-compliance with these principles. If residual risk remains, they must take further mitigating steps or accept the risk/s.

(18) Information Stewards provide support and advice for information management activities within their area.

(19) The Chief Information Security Officer oversees information security controls and responses to enable RMIT to deliver effective protection of data held by RMIT consistent with privacy and corporate management obligations across all its operations.

(20) The Chief Data and Analytics Officer (CDAO) is accountable for leading the information governance framework across RMIT and the CDAO team is responsible for enterprise information management standards in accordance with applicable legislation, under the Information Governance Policy.

(21) The Information Governance Board provides advice and recommendations for the strategy, policy and risk in relation to RMIT's information and data.

Compliance

(22) Breaches of this standard will be managed in accordance with the Compliance Breach Reporting Procedure.

Review

(23) The Chief Data and Analytics Officer will review this standard at least every three years in accordance with the Policy Governance Framework.

Status and Details

Status	Current
Effective Date	11th November 2020
Review Date	3rd September 2022
Approval Authority	Chief Financial Officer
Approval Date	21st October 2020
Expiry Date	Not Applicable
Policy Owner	Nonna Milmeister Chief Data and Analytics Officer
Policy Author	Henrique Delamanha Mendonca Director, Data Management and Governance
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).