Information Classification and Handling Procedure

Section 1 - Context

(1) This procedure provides guidance for individuals on how to:

a. handle RMIT Group data and information, referred to hereafter as 'Information'
b. apply the appropriate Information Classification in accordance with the Information Classification Standard
c. enable compliance with relevant RMIT policies including the Privacy Policy and the Information Technology and Security Policy, as well as statutory and regulatory requirements.

(2) According to the Information Governance Policy, an individual assumes the role of an Information Custodian when RMIT Information is in their possession. Information Classification provides a mechanism for Information Custodians to meet specific responsibilities and accountabilities to protect Information in their custodianship.

Section 2 - Authority

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

Section 3 - Scope

(4) This procedure applies to all RMIT Group Information, in all formats, as defined in the Information Governance Policy, except Information related to Australian national security and defence.

(5) This procedure applies to all individuals who create, use, manage, handle or process RMIT Group Information, including RMIT Group staff, casual employees, contractors, visitors, honorary appointees and third parties.

(6) The RMIT Group is RMIT University and its controlled entities, referred to hereafter as RMIT.

Section 4 - Procedure

Overview

(7) RMIT is legally and contractually obliged to manage its Information. Classification enables Information to be managed properly throughout its lifecycle, in accordance with legislative compliance and RMIT policy. It protects Information from unauthorised access, use and disclosure, and supports openness and collaboration.

(8) Information Classification provides context for information management and security. Provision and protection of Information in digital format is defined according to role-based access controls established by the Information Technology and Security Policy, which address baseline cyber security requirements for managing access on an approved, need-to-know basis.

(9) Individuals are responsible for understanding what constitutes Information Custodianship at RMIT, as defined by the Information Governance Policy, and for the proper treatment of Information across its lifecycle, as outlined in the Data and Information Lifecycle Management Procedure.

Information Handling

(10) Handling and protecting Information must occur whether Information is at rest or in use.

a. 'At rest' includes Information stored in databases, tables, email systems, file cabinets, desk drawers, etc.
b. 'In use' includes Information being processed by application systems, electronically transmitted, used in spreadsheets, or manually manipulated, etc.

(11) Handling and protecting Information depends on its Information Classification, physical and cyber security requirements, context and risk. The table below provides some recommendations for the handling of Information based on Security Classification.

Classification	Handling recommendations
Level 0 – Public	• Ensure Information accuracy and consistency
Level 1 – Trusted	• Physical security (e.g. locked bag) • No communication in public or via social media • Role-based access controls with at least yearly review cycle • Data sharing agreements with third parties • Third party non-disclosure agreement (NDA) • Data encryption at rest, if in digital format
Level 2 - Protected	• Physical security (cannot leave RMIT premises) • No staff communication in open spaces • Role-based access controls with at least quarterly review cycle • Data sharing agreements with third parties • Third party non-disclosure agreement (NDA) • Strong data encryption in transit and at rest • Data not used to train Artificial Intelligence (e.g; large language models)
Level 3 - Restricted	• Strict physical security (limited to prescribed spaces) • Staff communication limited to prescribed spaces • Role-based access controls with active cyber security monitoring • Strong penalty clauses for breach in data sharing agreements with third parties • Strong penalty clauses for breach in third party non-disclosure agreement (NDA) • Strong data encryption in transit and at rest • Data not used to train Artificial Intelligence (e.g; large language models)

(12) Information in non-digital format must be handled with equivalent levels of diligence as Information in digital format.

(13) Where it is feasible, duplicating of Information should be avoided and Information containing Personally Identifiable Information (PII) should be de-identified.

Information Classification

Part 1: Mandatory Security Classification

(14) Information Custodians should refer to Schedule 1 for definitions and examples of Security Labelling.

(15) Information Custodians should take care in applying the appropriate Security Label as there are implications for having an unreasonable security classification:

a. Under-classification may expose RMIT to risk if Information Custodians have not allocated sufficient security

resources to the Information.

b. Over-classification may devalue Security Classification overall, add administrative arrangements and security costs, and the Security Classifications may be ignored by individuals.

(16) The application of Security Labels is a two-step process:

a. Step 1 – Determine if the Information requires Security Labelling. Information that was obtained, generated or received for RMIT purposes or to support RMIT purposes (Institutional Data and Research Data) must have a Security Label.
b. Step 2 – Determine Security Labelling of the Information. Consider the impact to RMIT from the compromise, loss, or unauthorised disclosure of this Information. Refer to the Risk Consequence Tool to make this assessment. Consider whether custodianship of the Information Asset should be shared.

(17) In general, the most confidential Information element determines the Security Classification of the Information.

Part 2: Optional Management Classification

Internal Governance

(18) Management Classifications are metadata that enable the proper management of Information across the Information lifecycle. These metadata designations are optional and assist RMIT to identify Information, subject to internal governance, personal privacy, legal privilege, and/or records management obligations.

(19) A Management Classification may be applied to Information to distinguish which RMIT policy it is governed by. Parts A, B and C of the Data and Information Lifecycle Management Procedure define the governance and lifecycle of RMIT Information as follows:

a. Institutional Data is governed by the Information Governance Policy.
b. Research Data is governed by the Research Policy.
c. Unofficial Information is governed by the Acceptable Use Standard, Information Technology and Security Policy.

Personal Privacy and Legal Privilege

(20) A Management Classification may be added to identify Information subject to obligations under the Privacy Policy.

(21) A Management Classification adds context and helps differentiate between confidentiality requirements for Security Classification and obligations outlined in the Privacy Policy. For example:

a. Academic staff may have contact details such as an email address on the RMIT website. The Security Classification for the webpage may be Public even though it contains Personally Identifiable Information (PII) which traditionally requires a higher level of Security Classification.
b. Via role-based access control, colleagues within the same team are both authorised to handle Information containing Personally Identifiable Information (PII). Emails between these colleagues containing PII may be sent with the Trusted Security Classification, rather than the Protected Security Classifcaton in some contexts.

(22) A Management Classification may be applied to identify Information under Legal Privilege.

Public Records Compliance

(23) RMIT University is a public institution and must comply with the Public Records Act 1973. A Management Classification may be applied to enable records management compliance and the identification of Institutional Data and Research Data subject to retention classes in Section 5 of the Records Retention and Disposal Standard.

Institution Data Information Domain

(24) A Management Classification may be applied to identify the Information Domain of Institutional Information and Information Trustee(s) accountable for the Information.

Section 5 - Definitions

(Note: Commonly defined terms are in the RMIT Policy Glossary. Any defined terms below are specific to this policy document).

Handling Information	'Handling' Information in digital and non-digital formats includes, but is not limited to, the creating, collecting, accessing, viewing, using, storing, transferring, mailing, managing, preserving, disposing, or destroying that Information.

Status and Details

Status	Current
Effective Date	6th June 2024
Review Date	14th March 2028
Approval Authority	RMIT University Council
Approval Date	5th June 2024
Expiry Date	Not Applicable
Policy Owner	Teresa Finlayson Chief Operating Officer
Policy Author	Nonna Milmeister Chief Data and Analytics Officer
Enquiries Contact	Data Management and Governance

Glossary Terms and Definitions

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