Destruction of Information Procedure

Section 1 - Context

(1) As a public institution under Victorian law, RMIT must comply with standards issued by the Public Records Office Victoria (PROV) under the Public Records Act 1973. These mandatory standards apply to information in all formats and storage locations.

(2) RMIT must retain the information it creates as specified in the RMIT Retention and Disposal Authority (RDA). The RDA provides minimum, mandatory retention periods. Once the information reaches its minimum retention period and is eligible for destruction, it must be destroyed following the requirements in this procedure.

(3) Information may be retained longer than the prescribed mandatory minimum period providing the risks and costs associated with over retention can be justified.

(4) This procedure provides requirements for undertaking a destruction process using the RDA as well as using normal administrative practice (NAP).

Section 2 - Authority

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

Section 3 - Scope

(6) This procedure applies to all RMIT Group staff, students, temporary employees, contractors, visitors and third parties who manage RMIT information, except for research data as defined by the Research Policy.

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

(8) This procedure provides high-level requirements that must be met to undertake destruction of digital data records or information, regardless of storage location. It does not provide system-specific considerations and instructions. Each destruction process must implement these requirements in a way that minimises risk.

(9) This procedure does not apply to hardcopy data, records or information. For questions regarding the disposal or destruction of hardcopy records and information, please contact the Archives Team: archives@rmit.edu.au.

Section 4 - Procedure

Requirements for the Destruction of Information

Legal Requirements

(10) Destruction of information must be conducted in a lawful manner.

(11) It is unlawful to remove, sell, damage (either purposefully or by neglect) or destroy information without authorisation or following due process. This includes:

a. destroying information knowing that a document is or is likely to be required in evidence in a legal proceeding
b. destroying information subject to a request for access under the Freedom of Information Act 1982, which must not be disposed of until the request has been finalised and any appeal period has lapsed.

Authorisation

(12) Destruction of RMIT information must be authorised.

(13) The Retention and Disposal Standard must be referenced to ensure information is eligible for destruction i.e. has reached its mandatory minimum retention period.

(14) Internal authorisation must be sought prior to destruction. Destruction of RMIT information must only occur in accordance with this procedure, or via Normal Administrative Practice (NAP).

Informed Decision Making

(15) Destruction actions must be based on an informed decision-making process.

(16) Authorised destruction actions are determined through an informed decision-making process.

(17) Information destruction must be monitored to ensure it has been undertaken accurately.

Justification

(18) Destruction actions and retention periods for information must be justified.

(19) The University must be able to evidence that implementation of destruction decisions was authorised and lawful. Documentation must include:

a. relevant classes from the Retention and Disposal Standard
b. a full description of the information being destroyed
c. a record of all approvals, and
d. assurance/statement of destruction.

Planning

(20) Destruction of RMIT information must be planned, regular and integrated into the University's business processes and programs.

(21) Destruction of information must be a routine and integrated part of the University's overall information governance program to enable destruction to be carried out in a planned and systematic way.

Timeliness

(22) RMIT information must be destroyed in a timely manner.

(23) Temporary information must be destroyed as soon as practicable if it has met minimum retention periods as per the RDA.

(24) Prior to implementing destruction, the University must check that the information is no longer required for any other justifiable purposes I.e. business needs (which might include analytics purposes), legal or FOI requirements.

Security

(25) Destruction of information must be secure and irreversible so that it isn't inadvertently released or lost.

(26) Destruction should be undertaken with a level of security commensurate to the information security classification of the information.

Responsibilities

(27) All decisions relating to the destruction of information must be approved and overseen by RMIT employees with the appropriate delegations, as defined in the Public Records Act 1973 and outlined below.

(28) The Chief Data and Analytics Officer oversees information governance at RMIT University, which includes the destruction of data and information.

(29) Any staff member who has custody and responsibility over certain bodies of information at RMIT can propose information for destruction and is responsible for:

a. initiating the destruction process by identifying information for destruction and completing a proposal for destruction in line with the requirements described above.
b. obtaining required approvals for the destruction.
c. ensuring decisions and the destruction are documented and the documentation retained.
d. engaging other RMIT teams for review if required (i.e., Legal Services and Freedom of Information team)

(30) Information Trustees (as defined in the Information Governance Policy) are accountable for reviewing and approving information destruction.

a. The Information Trustee brings a knowledge of the high-level functions and goals of their area and makes a judgement as to the reasonable likeliness of current and future requirement for the information.
b. If the Trustee decides not to approve destruction, they must provide justification for its further retention and document the reasons for ongoing business need.

Normal Administrative Practice

(31) A normal administrative practice (NAP) is a process that allows staff to destroy certain types of low-value and short-term information in the normal course of business. Business information that is not needed to document our tasks and activities can be destroyed in accordance with a NAP without formal permission via the RDA.

(32) NAP reduces the retention of unnecessary information and consequently saves on storage costs. It is an important tool for the University to manage information efficiently and accountably.

(33) There are three instances where NAP applies:

a. working documents consisting of rough notes and calculations used only as a means to assist in the preparation of other information
b. drafts not intended for retention, the content of which has been reproduced and incorporated into the University's recordkeeping system or other system of record
c. additional copies of documents, emails and publications maintained for reference purposes.

(34) Categories and examples of NAP

Categories of NAP	Examples

Working documents consisting of rough notes and calculations used only as a means to assist in the preparation of other information such as correspondence, reports and statistical tabulations	Working documents include: 1. routine or rough calculations 2. working papers or background notes used to develop drafts 3. spreadsheets or word processing documents that have been incorporated into correspondence or a separate final document 4. system printouts or versions used to verify data or answer queries that are not part of regular reporting procedures and are not required for ongoing use.
Drafts not intended for retention the content of which has been reproduced and incorporated into the University's recordkeeping system or other system of record	Drafts that: 1. do not contain significant or substantial changes or annotations 2. are not required to document business activities.
Additional copies of documents, emails and publications maintained for reference purposes.	Copies: 1. documents, emails or other information that has already been saved into the University's records management system or system of record 2. duplicates of publications and promotional material. The area responsible for a publication is responsible for keeping a master copy. Externally published material and unofficial information 1. promotional or advertising material sent to the University 2. external publications and catalogues 3. unsolicited letters offering goods or services 4. unsolicited email (spam) 5. unofficial personal email.

Section 5 - Definitions

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

Recordkeeping	The 'making and maintaining of complete, accurate and reliable evidence of business transactions in the form of recorded information'.
Disposal	The range of processes associated with implementing appraisal decisions which are documented in disposal authorities or other instruments. These include: 1. the retention, destruction or deletion of records in or from recordkeeping systems 2. the migration or transmission of records between recordkeeping systems 3. the transfer of ownership or the transfer of custody of records (for example, to PROV) The lawful disposal of records is an essential and critical component of any records management program.
Destruction	The process of eliminating or deleting records, beyond any possible reconstruction.

Status and Details

Status	Historic
Effective Date	26th March 2021
Review Date	26th March 2024
Approval Authority	Chief Financial Officer
Approval Date	25th March 2021
Expiry Date	8th February 2024
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).