Destruction of Information Procedure

Section 1 - Context

(1) This procedure provides requirements to ensure Information is destroyed pursuant to obligations in the Public Records Act 1973.

Section 2 - Authority

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

Section 3 - Scope

(3) This procedure applies to RMIT Group staff, students, temporary employees, contractors, visitors and third parties who create, use, manage, handle or process data and information defined by Part A (Institutional Data) or Part B (Research Data) of the Data and Information Lifecycle Management Procedure.

(4) In addition to this procedure, destruction of Research Data must follow requirements in the Research Data Management Plan.

(5) Data and Information defined in Part C (Unofficial Information) of the Data and Information Lifecycle Management Procedure is not in the scope of this procedure and authority for its destruction sits with the Chief Information Officer (CIO).

(6) This procedure should be read in conjunction with the Retention and Disposal Standard.

Section 4 - Procedure

Requirements for the Destruction of Information

Legal Requirements

(7) Destruction of RMIT Records is conducted lawfully from either of the following:

a. Destruction of records under the principle of Normal Administrative Practice (NAP), defined below.
b. Destruction of records covered by a RMIT Retention & Disposal Authority (RDA), defined below.

(8) Records which have a retention period specified in the RMIT RDA may be destroyed when the records meet all conditions below:

a. Records have met the minimum retention period specified in the RMIT Retention and Disposal Authority (RDA), within the Retention and Disposal Standard.
b. Records are reasonably unlikely to be needed in a current or future legal proceeding. This includes any civil or criminal proceeding or an inquiry where evidence may be given before a court or person acting judicially, such

as a Royal Commission or Board of Inquiry.

c. Records are not required for meeting any Freedom of Information Act (FOI) applications which are not yet finalised.
d. Records are not required for audits or investigations which are not yet finalised.

Business Requirements

(9) Destruction of RMIT records must be planned and integrated into the University's business processes and programs, including information governance.

(10) Records designated for destruction must no longer be required by the responsible work unit, school or college, or for any other justifiable business or operational purpose.

Authorisation

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

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

(13) Destruction of RMIT records must be authorised.

(14) Internal authorisation must be sought prior to destruction.

Documentation

(15) 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 Authority (RDA)
b. a full description of the information being destroyed
c. a record of all approvals, and
d. assurance/statement of destruction. Refer to the RMIT Destruction of Information Data Template for more information.

Timeliness

(16) Once authorised, records must be disposed of or destroyed in a timely manner.

Security and Irreversibility

(17) Destruction should be undertaken with a level of security commensurate to the Information Classification of the record.

(18) Records destruction must be monitored to ensure it has been undertaken accurately.

(19) Destruction of records must be secure and irreversible such that records be inadvertently released or lost.

Destruction of records under Normal Administrative Practice (NAP)

(20) Records which can be destroyed via Normal Administrative Practice (NAP) principles are not subject to the retention requirements in the RDA, are pre-authorised for destruction and do not require documentation.

(21) NAP allows for the destruction of:

a. working documents, such as notes or calculations, used to assist in the preparation of other records and

duplicate copies.

b. minor drafts and transitory documents, where the content is reproduced elsewhere, and the information will not be needed to show how the work has progressed or actions approved.
c. minor updates of content, such as those in databases, which will not be needed to show actions, decisions, or approvals.

Destruction of records under a Retention and Disposal Authority (RDA)

(22) Requirements for the Destruction of Information must be met and documented this via the RMIT Destruction of Information Data Template.

Responsibilities

(23) 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.

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

(25) 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)

(26) 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.

Section 5 - Definitions

For the purposes of this procedure:

Record	Is a set of information created, collated, received, or maintained as evidence while conducting the business of RMIT and/or in pursuance of legal obligations.
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	Current
Effective Date	9th February 2024
Review Date	14th March 2028
Approval Authority	Senior Policy Advisor
Approval Date	6th February 2024
Expiry Date	Not Applicable
Policy Owner	Nicola Burgess Interim Executive Director, Technology
Policy Author	Chloe Sanford Director, Engagement & Enablement
Enquiries Contact	Data and Analytics