

## Records Management Policy and Procedure

### 1. Purpose

The purpose of this policy and procedure is to:

- support the effectiveness and efficiency of the Institute’s operations and quality assurance;
- facilitate legislative and regulatory compliance;
- protect Institute information as evidence of current practice; and
- capture corporate memory.

### 2. Scope

This policy and procedure will apply to all organisational units, all staff and all functions of the Institute.

### 3. Definitions

Term	Definition
Group General Manager	means the person holding the position of Group General Manager within the Institute or nominee.
Metadata	means a set of data that describes and gives information about other data.
Permanent value records	means records that have been identified by the Institute as being worthy of preservation or having historical significance.
Record	means any information, in any format (electronic, paper, image) that is created, received, used or maintained by staff of the Institute whilst conducting Institute activities.
Records Management	means field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. (Source: AS ISO 15489.1 - 2002)
RDA	means a records disposal authority.
Student records	means records of each accepted student who is enrolled with the Institute or who has paid any tuition fees for a course provided by the Institute.

---

**Warning: uncontrolled when printed.**

Original Issue:	17 November 2017
Last reviewed by the Policy Committee (PC):	16 November 2021
Approved by the Executive Management Committee (EMC):	12 March 2020
Endorsed by the Board of Directors (BOD):	27 March 2020
Reviewed policy is effective from:	27 March 2020
Review date:	11 March 2025

#### 4. Policy Statement

- 4.1. The Institute creates, captures and maintains full, accurate, up-to-date records of its activities, including outsourced, contracted or cloud-based activities. All areas of the Institute's operations must keep records in accordance with this policy, on matters such as learning and teaching, engagement, research, administrative operations and commercial activities. The Institute will also maintain records relating to students' complaints and appeals.
- 4.2. The Institute will apply good recordkeeping principles when creating, capturing, maintaining and disposing of Institute records. Institute records represent accountability and corporate memory and are important for accurate reporting, auditing and enquiries.
- 4.3. Institute records can be in any format (electronic documents, hardcopy, letters, e-mails, spread sheets, legal contracts and agreements, building plans, photographs, etc.) and are the property of the Institute and subject to Privacy and other legal requirements to do with the keeping of records.
- 4.4. All staff should be aware of the need to protect Institute records from neglect, premature destruction and inappropriate disclosure or access. All staff must capture, maintain, archive or destroy Institute records in accordance with this policy and procedure.
- 4.5. Student records must contain:
  - application for admission;
  - the student's current residential address;
  - the student's mobile phone number (if any);
  - the student's email address (if any); and
  - all written agreements and payments made by the student;
  - evidence of meeting course entry requirements;
  - passport (international students only);
  - any requests for letters of release and the process used to make a decision in relation to the request;
  - any intervention strategies;
  - all significant communication or advice;
  - any action taken in regard to a critical incident involving the student, including outcomes or evidence if the incident is referred to another person or agency;
  - details of Credit Transfer (CT) or Recognition of Prior Learning (RPL) granted to the student. The records of the CT or RPL decision and the written record of acceptance are to be retained for a minimum of two years after the student ceases to be an accepted student.
  - details of student transfers granted to, or refused to, a student. The records of the transfer decision are to be retained for a minimum of two years after the student ceases to be an accepted student. This includes applications for transfer and letters of acceptance or refusal to the student.
  - details of student complaints and appeals. The records of the complaint or appeal, correspondence with students and all other relevant records are to be retained for a minimum of two years after the student ceases to be an accepted student.
  - Qualification and achievement documentation issued to the student.
  - any other details required under the relevant ESOS Standards of the National Code and/or the ESOS Act.

---

**Warning: uncontrolled when printed.**

Original Issue:	17 November 2017
Last reviewed by the Policy Committee (PC):	16 November 2021
Approved by the Executive Management Committee (EMC):	12 March 2020
Endorsed by the Board of Directors (BOD):	27 March 2020
Reviewed policy is effective from:	27 March 2020
Review date:	11 March 2025

## 5. Procedure

- 5.1. Records must be organised and managed to preserve their context and ease of retrieval.
- 5.2. Records must be stored in conditions suitable to the:
  - length of time they must be kept;
  - nature of the record content (e.g. personal, confidential or sensitive information);
  - format of the record or the medium it is kept on.
- 5.3. Records must be maintained on Institute business management records systems or infrastructure that is capable of meeting records management standards and legislative requirements.
- 5.4. A system must be assessed for compliance with records standards before it is implemented or before records are migrated to or from the system. A major change to an existing system must also be assessed for such compliance.
- 5.5. The Institute's business emails and their attachments must be retained.
- 5.6. Access to Institute records will only be permitted to staff authorised by the Group General Manager. Records may only be made available to authorised people or organisations outside of the Institute in accordance with legislation and within the constraints of security, confidentiality, privacy and archival access conditions.
- 5.7. Institute records that may be disposed of by staff include:
  - working documents, notes used only to assist in the preparation of other records such as reports, and correspondence;
  - drafts not intended for retention;
  - additional copies of documents, emails or publications.
- 5.8. Subject to 5.7, all other records no longer required for normal business activities must be assessed by the Group General Manager who will determine if they can be disposed of under RDA.
- 5.9. Records must be disposed of in accordance with a RDA, using secure and permanent methods unless there is:
  - a pending or anticipated legal action or business use;
  - a current hold or freeze on destruction issued by the Group General Manager.
- 5.10. Permanent value records will be transferred to the Institute archives for preservation and access.
- 5.11. Staff must not:
  - Mislaid records that they are responsible for;
  - Remove hardcopy records from the relevant department without permission;
  - Disclose confidential or sensitive Institute information to unauthorised parties.
- 5.12. The Office of Administration and Experience will ensure that, at least every six- months, while a student remains an accepted student of the Institute it confirms, in writing, the details referred to in section 4.5, with the student and that the records are updated accordingly.

---

**Warning: uncontrolled when printed.**

Original Issue:	17 November 2017
Last reviewed by the Policy Committee (PC):	16 November 2021
Approved by the Executive Management Committee (EMC):	12 March 2020
Endorsed by the Board of Directors (BOD):	27 March 2020
Reviewed policy is effective from:	27 March 2020
Review date:	11 March 2025

### 5.13. Guidelines for record retention:

Type of record	Retention period
Company records including metadata	7 years after administrative use has concluded, unless retained for business use
Employee records	5 years or once administrative use has concluded
Student records and student administration including incident reporting and complaints, student assessments, appeals, academic misconduct cases, course development and third party arrangements	External regulations and legislation (ESOS Act, TEQSA Act and national Code) require student records to be retained for a minimum of 2 years from when the student ceases to be an accepted student of the Institute. MIT practice is to retain these records online for a period of at least 7 years from when the student ceases to be an accepted student of the Institute.
Student academic transcripts and testamurs	Archive as permanent value records

## 6. Responsibilities

6.1. The Group General Manager has oversight of the Institute's records management system.

6.2. All staff are responsible for:

- creating, capturing, managing and disposing (where permitted) of records relating to their Institute duties;
- being aware of their responsibilities for protecting personal and confidential information when accessing Institute records;
- ensuring records in their custody are made available to the Institute when they leave the Institute.

6.3. Each department is responsible for boxing its own physical records, where they are designated for retention, and for storing them as directed by the Group General Manager.

## 7. Implementation and communication

This policy and procedure will be implemented and communicated through the Institute via:

- the Institute's website;
- Internal circulation to staff;
- as part of Staff professional development and meetings.

## 8. Legislation

Crimes Act 1958 (Vic)

Health Records Act 2001 (Victoria)

Health Records and Information Privacy Act 2002 (NSW).

ESOS Act 2000 (Cth)

### Other:

MIT Privacy Policy and Statement

---

### Warning: uncontrolled when printed.

Original Issue:	17 November 2017
Last reviewed by the Policy Committee (PC):	16 November 2021
Approved by the Executive Management Committee (EMC):	12 March 2020
Endorsed by the Board of Directors (BOD):	27 March 2020
Reviewed policy is effective from:	27 March 2020
Review date:	11 March 2025