MELBOURNE
INSTITUTE OF TECHNOLOGY

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;
- providing for evidence based and informed decision making;
- promoting accountability and transparency
- facilitate legislative compliance; and effective business practice;
- protect Institute information assets as evidence of current practice to support future business and research and
- capture corporate memory.

2. Scope

This policy and procedure and the schedules applies to:

- all organisational units, all staff and all functions acting in their official capacity for or on behalf of the Institute
- all campuses.
- all aspects of the Institute's business, including teaching and learning, research, student administration and services, governance and corporate/administrative services; and
- Institute records in all formats, including physical (hard copy or paper) records, digitized and scanned records, electronic records including email, records held in databases or on websites, and other technology-dependent records

This policy does not cover Research Data Management.

3. Definitions

Term	Definition
AMS	abbr. Academic Management System is an in-house purpose-built MIT policy governed Management System for students, and staff (administrative and academic) of the Institute to manage daily and term-based tasks.
Bigfoot	Bigfoot is an in-house purpose-built MIT policy governed student database / lifecycle management system.
Disposal	means a range of processes associated with implementing records retention, destruction, or transfer decisions, which are documented in the Institute Records Disposal Register.
ELO	(Toshiba) ELO is a purchased Document Management System, housed internally and programmed to the needs of MIT to be used as a student soft copy document repository.
Employee records	defined in the Privacy Act 1988 (Cth) as a record of personal information

Term	Definition
	relating to the employment of the employee.
FEE-HELP	is an Australian loan scheme that assists eligible fee-paying students to pay all or part of their tuition fees at university and other higher education providers.
Group General Manager	means the person holding the position of Group General Manager within the Institute or nominee.
Important records	Records that can only be reproduced at considerable expense, time and labour. Important records include: • Agendas, minutes and papers of governance committees • Student and staff files • Class results including enrolments, attendance records and results • Teaching materials including unit descriptions, lecture notes, assessment briefs, examination papers • MIT publications e.g. course guides, course information etc • Current calendars and timetables
International student	means a student on an Australian student visa.
Learning Management System (LMS) (Moodle)	a software application for the administration, documentation, tracking, reporting, automation and delivery of educational courses, training programs, materials or learning and development programs
Metadata	means a set of data that describes and gives information about other data.
Normal Administrative Practice (NAP)	means a process that allows the Institute to destroy certain types of low-value and short-term information in the normal course of business.
Permanent value records	means records that have been identified by the Institute as being worthy of preservation or having historical significance.
PRISMS	means the Provider Registration International Student Management System (PRISMS) – an Australian Government secure online system that allows providers to issue Confirmations of Enrolment (CoEs). PRISMS is used by government agencies to monitor student compliance with visa conditions and to monitor educator provider compliance with the ESOS Act 2000.
Record	means any information, in any format (electronic, paper, image) that is created, received, used or maintained as evidence he Institute in pursuant of legal obligations or in the transaction of business.
Records	means field of management responsible for the efficient and systematic

Term	Definition
Management	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 which sets out the requirements for the retention and destruction of Institute records and information, in line with legislative and business needs, as well as recordkeeping standards issued under the *Public Records Act 1973* (Vic).
Retention period	means the minimum period that records must be kept before they can be legally destroyed.
Staff records	Each staff member has a file created and maintained for the purpose of employment which include: • Recruitment paperwork • employment conditions/ letter of offer/ employment agreement • evidence of the right to work within Australia • position description • curriculum vitae or resume and application letter • evidence of participation in the staff induction process • certified copies of qualifications • verification of experience • professional development, scholarly activities and research
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. Records will be stored in MIT secure IT systems. Records include but not limited to: • Personal information • completed application forms and supporting enrolment documentation • confirmation of enrolment (Coe) for international students and signed agreements • details of payments and refunds • enrolment details including Credit/RPL applications and outcomes • special consideration forms • results for each assessment in a unit of study, final marks and grades • copies of testamurs and records of results • any student intervention activity or actions • any notes made by the academic and/or professional staff about the student (including disciplinary matters).
Temporary value record	means a record defined as temporary in the Institute's Records Retention and Disposal Authority, which is required to be kept for a minimum period of time for legislative or other requirements, before it can be destroyed.
Vital Records	Vital records include documents that: • Prove ownership of property, equipment, vehicles and products • Record how MIT operates

Term	Definition
	• Document governance decisions, policies, goals and planning • Document curriculum and course development • Any other records whose absence will severely impeded the function of MIT Examples of vital records include: • Deeds and certificates of title • Insurance policies • Contracts and agreements • Financial records • Minutes of the Board of Directors and the Academic Board • Proof of registration, certifications, approvals and accreditation of courses • Curriculum and course development records • Student data, including enrolment data, results, transcripts etc • Alumni data and the graduation register

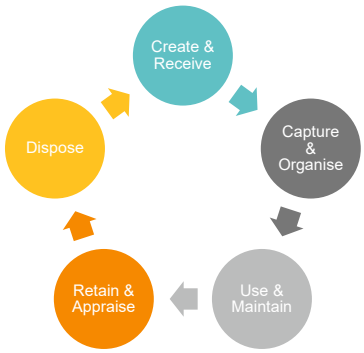
4. Policy Statement

4.1. Quality educational and research programs, and effective institutional administration, are dependent on the Institute creating and maintaining accurate and comprehensive records.

4.2. Records provide the Institute with a corporate memory, which enhances decision making, improves our ability to engage with students and stakeholders, and mitigates risk.

4.3. Records maintain evidence of actions and decisions, and safeguard the legal rights of students, stakeholders and the Institute. Managing these records well strengthens organisational accountability and supports the implementation of the Institute's Strategic Plan

4.4. MIT's record management program will be carried out with reference to the following principles



Adapted from James Cook University, Records Management Policy: https://www.jcu.edu.au/policy/university-management/corporate-administration/records-management-policy)

MIT Records have legal status and weight

4.5. All records created or received in the course of Institute business are the property of MIT.

4.6. Records must not be removed from MIT premises, deleted, destroyed or otherwise disposed of except in accordance with this Policy and its associated procedure.

4.7. In the event of a third party wishes to gain access to Student Records, written permission must be provided by the student, unless the request if made by subpoena.

Creation of Records

4.8. The Institute creates, captures and maintains full, accurate, up-to-date records of its activities, including outsourced, contracted or cloud-based activities.

4.9. 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.

4.10. All staff are responsible for creating accurate and complete records of their MIT related activities.

4.11. Records must be created to document all MIT related activities, decisions and commitments (including emails, oral decisions and outcomes of meeting or telephone conversations).

4.12. Records must be made at the time of, or as soon as practicable after, the event to which they relate.

4.13. The Institute will also maintain records relating to students' complaints and appeals.

4.14. The Institute will apply good record keeping 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.

4.15. 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 MIT's Privacy Policy and other legal requirements to do with the keeping of records.

4.16. 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.

4.17. Staff must not:

- Mislay 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. Procedure

Creation and storage of records

5.1. Records must be organised and managed to preserve their context and ease of retrieval using consistent naming conventions. See Schedule File Naming Conventions Guidelines

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.

Security

5.3. MIT takes seriously its obligations under privacy legislation to safeguard all confidential information. MIT will also ensure that anyone acting on its behalf maintains appropriate confidentiality.

5.4. It is a requirement that records are kept in a secure environment and safeguarded against loss, damage or unauthorised access. Only authorised staff will be granted access to student and staff records.

5.5. MIT maintains a secure computer network. Each user has their own password which allows them access to specific functions and files within the system as appropriate.

5.6. Records must be maintained on secure Institute business management records systems or infrastructure that is capable of meeting records management standards and legislative requirements.

5.7. 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.

5.8. The Institute's business emails and their attachments must be retained.

5.9. IT infrastructure is protected and secured in the following ways:

- Backups (including software as well as all data information) are sent off-site on a monthly basis to facilitate recovery.
- A remote backup facility if utilised to minimise data loss
- Surge protectors are employed to maintain the effect of power surges on electronic equipment
- Servers and essential equipment are protected by an Uninterruptible Power Supply
- An effective alarm system and accessible fire extinguishers are installed in case of a fire
- Antivirus software, firewalls and other security measures are employed
- Electronic records are backed up each night
- Backups are rotated daily
- The computer network is maintained by a programmed regimen of maintenance along with ad hoc support as and when required.
- Cloud based security MIT systems are used to protect against external intrusions; and
- Remote back-up systems are tested at least twice a year to ensure they are working.

Student records management

5.10. A separate file is created for each student in the Student Management System identified by student number.

5.11. Student records are maintained by the Registrar

5.12. Student records may be stored as digitised copies and saved to the MIT systems (ELO).

5.13. Student records must be identified by their individual Student ID number supplied by the

institute.

5.14. 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.

5.15. The Office of Student Administration and Engagement 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.

Staff records management

5.16. The Manager People and Culture maintains staff records in the Human Resource Information System (UKG).

5.17. Copies of original documentation including qualifications kept on file must be sighted to verify authenticity and indicate the date sighted and by whom (refer to the Academic and General Staff Recruitment Policy and Procedure).

5.18. Disciplinary action or details of grievances in which the staff member is a complainant or respondent may also be noted in the staff file (as per the Staff Complaint Policy and Procedure)

5.19. Staff may access information on their files through a written request to the Manager People

and Culture.

5.20. Third party access is only permitted when required by law or with the express and written permission of the relevant staff member.

Financial records management

5.21. Financial records are created, secured, retained and archived in compliance with contractual and legal requirements.

Retention

5.22. All documents are retained as per Schedule 1 of this document.

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 enrolled student of the Institute.
Student academic transcripts and testamurs	Archive as permanent value records

5.23. Refer to Schedule 1 accompanying this policy for details on the retention schedules for all documents.

Disposal

5.24. Records will be disposed of in accordance with the Australian Privacy Principles Guidelines for Information held by an organisation.

5.25. Where personal information is no longer required for any legitimate and sanctioned purpose, MIT will take reasonable steps to destroy and/or deidentify the information, together with any copies of the information including archived records and back-ups.

5.26. 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. (See Schedule 1)

5.27. Subject to 5.26 and Schedule 1 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 the RDA. (see Schedule 1 Storage and handling of different types of records).

5.28. Records must be disposed of in accordance with the RDA, using secure and permanent methods unless there is a :

- pending or anticipated legal action or business use;
- current hold or freeze on destruction issued by the Group General Manager.

5.29. Permanent value records will be transferred to the Institute archives for preservation and access.

6. Responsibilities

6.1. The Executive Management Committee take responsibility for risk assessment in relation to record keeping, taking decisions and implementing changes where needed to minimise risk and address hazards identified by staff

6.2. The GGM as per the Delegations Register has:

- oversight of the Institute's records management system
- managing any complaints about privacy and ensuring a written response is provided to the complainant as soon as possible
- the safe storage and handling of contracts, deeds, insurance policies
- the safe storage and handling of proof of provider accreditation, registration, certification, etc.
- monitoring the effectiveness of this framework within their scope of responsibility
- making recommendations with respect to this framework to appropriate personnel and committees.

6.3. The Associate Director Finance is responsible for the safe storage of finance and accounting records.

6.4. Finance Team are responsible for the safe storage and handling of student financial details and related student correspondence

6.5. The Director HR is responsible for:

- managing staff requests for access to their personal information or employee records
- the safe storage and handling of staff personal information or employee records
- the safe storage and handling of personal information or employee records of prospective employees or unsuccessful candidates
- the safe storage and handling of personal information or employee records of independent contractors
- the safe storage and handling of payroll records.

6.6. Campus directors are responsible for ensuring that:

- records storage areas for physical records under their control are secure and protected from accidental damage (such as fire, water, mould or vermin). This includes records stored in office areas.
- This policy is adhered to by all staff.

6.7. The Executive Dean is responsible for

- the safe storage and handling of student assignments and other assessed works

- the safe storage and handling of course details

6.8. The Heads of School are responsible for

- the safe storage and handling of student assignments and other assessed works
- the safe storage and handling of course details

6.9. The Software Development Division are responsible for maintaining MIT systems such as the Student Management System and Academic Management System that store and handling student details and academic administration.

6.10. Counsellors are responsible for the safe storage and handling of student counselling records.

6.11. All staff are responsible for:

- using consistent file naming conventions
- 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.
- maintaining accurate student records that relate to their School
- the safe storage and handling of student assignments and other assessed works; student correspondence including special consideration, extensions,

6.12. Each department is responsible for boxing its own physical records where appropriate, 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. Supporting documents and references

- Admission Policy
- Enrolments Policy
- Credit Transfer and Recognition of Prior Learning Policy and Procedure
- Feedback Policy
- Assessment Policy and Procedure
- Academic Integrity Policy and Procedure
- Moderation of Assessment Policy
- ELICOS Policy and Procedure
- User Account, Email and Internet Guidelines
- Notifiable Data Breach Policy and Procedure

- Staff Code of Conduct
- Staff Complaint Policy and Procedure
- Academic Appeals Policy and Procedure
- Domestic Student Acceptance of Offer, and Terms and Conditions of Enrolment, Fee Payment and Refund Policy
- Overseas Student Refund Policy and Procedure
- Student Academic Progress Policy and Procedure
- Student Complaints and Grievances Policy and Procedure
- Student General Misconduct Policy and Procedure
- Student Transfer Policy and Procedure
- Privacy Policy

Tertiary Education Quality and Standards Agency Act 2011 (TEQSA Act)
Higher Education Standards Framework (Threshold Standards) 2021
Education Services for Overseas Students Act 2000 (ESOS Act)
Education Services for Overseas Students Regulations 2019 (ESOS Regulations)
National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code)
ELICOS Standards 2018
Crimes Act 1958 (Vic)
Crimes Act 1900 (NSW)
Evidence Act 2008 (Vic)
Evidence 1995 (NSW)
Freedom of Information Act 1982 (Vic)
Freedom of Information Act 1989 (NSW)
Health Records Act 2001 (Victoria)
Health Records and Information Privacy Act 2002 (NSW).
Privacy and Data Protection Act 2014 (Vic)
Privacy and Personal Information Protection Act 1998
Australian Code for the Responsible Conduct of Research 2018
National Statement on Ethical Conduct in Human Research 2007 – Updated 2018
Code of Ethics for Aboriginal and Torres Strait Islander Research 2020
Public Records Act and all associated Public Record Office of Victoria Standards and the Australian Standard for Records Management, AS ISO 15489-2002;

Schedule 1: Retention of Student Records Schedule

1.1. Storage and handling of student records

Category	Source	Storage	Access	Security	Retention
Student Testamurs and Transcripts	Academic Board and BoD Decisions Conferral decisions and results ratifications	Digitised data in held in MIT systems	Academic Registrar and OSAE	Digital files held MIT systems with restricted password-protected access	Permanent – do not destroy
Records of ALL students, including where applicable for domestic and international students: • written agreement(s) between the student and MIT • Name and gender • Course, location, start date and expected duration of the	Course application forms and supporting documents	Digitised records are held in the MIT applications porta and transferred into ELO. Hard copies are stored in secure locked filing rooms that are accessible by CDs and nominated staff	Students may request in writing to the Academic Registrar with nominated staff providing information to students.	Digital files held in web- hosted student database with restricted password-protected access. Hard copies held in secure locked filing rooms that are accessible by CDs and nominated staff	Records are required to be retained for as long as MIT continues to provide services to that student and for seven years after that student ceases to be enrolled.

Category	Source	Storage	Access	Security	Retention
student's course at MIT • Date of birth, country of birth and nationality • date when the student is expected to complete their course at MIT • amount of tuition and non-tuition fees received before confirming the student's enrolment using PRISMS • total tuition fees required to be paid to undertake full course • whether premiums have been paid for					

Category	Source	Storage	Access	Security	Retention
student health insurance before the course commences current residential address • mobile phone number (if any) • email address (if any) • amount to be charged for the student to access their records (if applicable), and • up-to-date records of assessment. • details of person who has legal authority to act on the student's behalf (if the					

Category	Source	Storage	Access	Security	Retention
student is under 18 years old) • IELTS/PTE certificates					
Student financial records including: • the total amount of fees • payment terms • any non-refundable deposit or administration fee and • fees and charges for additional services • Scholarship granted	Scholarship application forms and supporting papers, documents indicating decisions, copies of financial transactions	Individual student applications and associated documentation are held in JDrive or digital electronic records on ELO. Hard copies are stored in secure locked filing rooms that are accessible by CDs and nominated staff	Hard copies: student in Administrator's presence, staff as needed for duties. Electronic data: Key staff in student and academic administration teams and finance can access documents as needed.	Hard copies held in secure locked filing rooms that are accessible by CDs and nominated staff Access to student management system has levels of security, with change rights being restricted to key staff approved by the Academic Register.	Records are required to be retained for as long as MIT continues to provide services to that student and **for seven years** after that student leaves MIT.
Academic details (enrolment, attendance and assessment details	Forms created on MIT systems (some	Individual student records held in secure filing rooms	Students may request in writing to the Academic	Hard copies held in secure locked filing rooms that are	Records are required to be retained for as

Category	Source	Storage	Access	Security	Retention
related to student's progress through the course	manually completed), printed testamurs	or as. electronic records on MIT secure systems	Registrar who will delegate to nominated staff to provide information. Digital Class files available on Moodle accessed by delegated professional and academic staff as needed for duties	accessible by CDs and nominated staff Access to the student management system has levels of security, with change rights restricted to key staff in student academic and financial administration. Class files are sighted by nominated staff as needed through Moodle.	long as MIT continues to provide services to that student and for **seven years** after that student leaves MIT.
Individual assessment components of a unit and determination of final results/grades. Includes: • examiners/assessor's reports and related	Student-generated work in hard copy and/or softcopy submitted through MIT systems	Unmarked and Marked Exam and Test scrips are held in locked locations and signed out to the academics as	Heads of Schools, academic staff, Academic Registrar and professional staff.	Hard copies held in secure locked filing rooms that are accessible by CDs and nominated staff.	Records are required to be retained for as long as MIT continues to provide services to that student

Category	Source	Storage	Access	Security	Retention
records for HDR students • appeals of grades • local school level informal requests for extension of assessment components for a unit • local special consideration arrangements		required by academic services staff. Other assessments are housed and marked in Moodle.		Academic papers and data, HDR thesis and data are stored in the Research Repository maintained by the MIT Library Managers	and for **seven years** after that student leaves MIT.
Student grievances, complaints and misconduct record and evidence	Student Grievance application and supporting documentation, supplemented with other relevant student records	Mainly digitised and held electronically	Academic Register and nominated staff and committee members	Access if controlled by the Group General Manager who may provide access to nominated staff	**Seven years** from the date the complaint or appeal was lodged
FEE-HELP application documentation	Forms created on MIT systems (some manually completed),	Mainly digitised and held electronically	Academic Registrar's and Finance	Access if controlled by the Group General Manager who may	Records are required to be retained for as

Category	Source	Storage	Access	Security	Retention
				provide access to nominated staff	long as MIT continues to provide services to that student and for seven years after that student leaves MIT.
Records required for legal action	Letters, emails, file notes, student and staff complaints and grievances, appeals and supporting documentation supplemented with other relevant student or staff records	Mainly digitised and held electronically	Group General Manager HR Director and nominated staff	Access if controlled by the Group General Manager who may provide access to nominated staff	Retained until the completion of that legal action, including appeals.
Student transfer requests Internship applications Variation in enrolment load that may affect students' duration of study course progress Attendance	Forms created on MIT systems (some manually completed), Credit/RPL applications, Internship applications and supporting documentation, Critical	Mainly digitised and held electronically.	Electronic data base student academic and financial administrators only.	Group General Manager/ Academic Registrar Campus Directors, OSAE staff, Admissions and Marketing	Records are required to be retained for as long as MIT continues to provide services to that student and for seven

Category	Source	Storage	Access	Security	Retention
Course credit / RPL applications Applications for deferment or suspension A written record of any critical incident and remedial action taken	incident reports, Letters, emails, file notes, electronic data on database				**years** after that student leaves MIT.
Personal Counselling records	The following documents (designated counselling in nature) are to be marked as confidential including but not limited to Medical Reports (including physical health and psychological reports), confidentiality consent forms, personal statements (for appeals), support letters, case notes, care plans, legal documents, risk assessments,	Held in locked, coded files in Counsellor Filing cabinets Scanned documents are housed in MIT's digital document management system (ELO)	Hard copies can only be accessed by counsellors Electronic records are accessed by Campus Directors and Counsellors only.	Access is controlled by the Group General Manager Physical cp	Records are required to be retained for as long as MIT continues to provide services to that student and for **seven years** after that student leaves MIT.

Category	Source	Storage	Access	Security	Retention
	police reports, complaints containing sensitive or confidential information and referrals to other services.				
Learning Support Plans	Forms created on MIT systems (some manually completed Medical or health records	Digitised and held electronically	Campus Directors and COL staff	Access is controlled by Campus Director	Records are required to be retained for as long as MIT continues to provide services to that student and for **seven years** after that student leaves MIT.

1.2. Storage and handling of student archives

Category	Source	Storage	Access	Security	Retention
Research Records (documents, correspondence, materials and data generated during research undertaken by MIT researchers and research students.	Final approved theses, compilations and/or creative equivalents for assessment for Master of Research qualifications Research data and materials including questionnaires, audio and video recordings, images, test results, transcripts, laboratory notes, algorithms and coding scripts databases or data sets.	Library Repository for digital records	Delegated staff and researchers	Access is controlled by Library Managers.	Permanent – do not destroy
Academic results for each unit	Hard copy files containing attendance records, results, unit	Stored online in learning management	Academic Register and nominated staff as needed for duties	Archive room is kept locked, with keys held by Academic	Records are required to be retained for as long as MIT

Category	Source	Storage	Access	Security	Retention
	outlines and student feedback. Student results also held electronically in student management system	system. Older documents stored in locked storage areas across campus facilities		Services and/or Master Key holders. Student management system access is by individualised security permissions	continues to provide services to that student and for **seven years** after that student ceases to be enrolled.
Student personal files	Student files containing complete personal information and academic history	Older files are kept in archive storage. Otherwise all personal files are kept online in student database	Academic Register and nominated staff as needed for duties	Archive room is kept locked, with keys held by Academic Services and/or Master Key holders. Student management system access is by individualised security permissions	Records are required to be retained for as long as MIT continues to provide services to that student and for **seven years** after that student ceases to be enrolled.
Student administration archives	Handbooks; graduation files	Older files are kept in archive storage. Otherwise kept online on JDrive	Academic Register and nominated staff as needed for duties	Archive room is kept locked, with keys held by Academic Services and/or Master Key holders. JDrive access is by individualised security	Records are required to be retained for as long as MIT continues to provide services to that student and for **seven years** after

Category	Source	Storage	Access	Security	Retention
				permissions authorised by the GGM	that student ceases to be enrolled.

1.3. Storage and handling of Staff Records

Category	Source	Storage	Access	Security	Retention
Personnel files/employee records	All employment documents, including contracts, curriculum vitae, certified qualifications, position descriptions, reviews, WWCC, Police checks etc Staff Complaints and Grievances	Staff personal information is saved and backed up on SharePoint and UKG (HRIS) Personnel folders and archive folders are held in locked cabinets in the archive room and in offices	Management staff as needed for duties	J Drive access is by individualised security permissions. Files of former staff held in locked storage (archive room), locked office cabinets	Records must be kept for a minimum of 7 years
Payroll records	Staff contracts and online forms	Staff personal information is saved on AMS and UKG (HRIS). Personnel folders and achieve folders are held in locked cabinets in the archive room and in offices	Individual staff access to personal information on UKG using password protection. Managers have access to team members information on UKG using password protection CD, SDD and staff authorised by GGM can access	Password-protected access Access rights based on security settings	Records must be kept for a minimum of 7 years

Category	Source	Storage	Access	Security	Retention
			sessional contracts on AMS.		
Recruitment records	CVs, interview guides and assessment tasks	Saved and backed up on JDrive and MIT HRIS	People and Culture staff and Recruitment Committee	JDrive and UKG access is by individualised security permissions	Records must be kept for a minimum of 7 years

1.4. Storage and handling of course materials

Category	Source	Storage	Access	Security	Retention
Course details – structures and curricula	Course accreditation documents	JDrive	Head of School, CC, Professional Staff	JDrive with restricted access.	Permanent – Do not destroy
Course details – course information books	Compiled publications	Electronically on Jdrive. Also published as printed booklets. All formats controlled by issue and date	Digital copies available on website. Hard copies available onsite and on request	Original digital files held in JDrive with restricted access authorised by GGM Digital files published and updated on website	Permanent – Do not destroy
Course materials – study guides, readers, etc.	ED, Heads of School, Academic staff, Academic Administrative staff	Held electronically on J Drive and uploaded to the learning management system.	Available to enrolled students and teaching staff. Copyright restrictions on use.	Original digital files held and updated in School's JDrive folder with restricted access. Published in digital format on the learning management system	Permanent – Do not destroy

1.5. Storage and handling of other vital documents

Category	Source	Storage	Access	Security	Retention
Contracts, deeds, insurance policies	Signed/authorised documents which may be received electronically or in print.	Electronic versions stored on JDrive Hard copy originals held in locked cabinet in secure offices.	Chief Executive, delegated management staff or nominees as required.	Digital files held in JDrive with restricted access Hard copy originals held in cabinet onsite	Permanent – Do not destroy
Financial records	Digital records Hard copies of invoices, receipts, contracts	Electronic versions stored on J Drive Hard copy originals held in locked cabinet in secure offices.	Finance staff	Digital files held in JDrive with restricted access Hard copy originals held in cabinet onsite	Records must be kept a minimum of 7 years.
Proof of provider accreditation, registration, certification, etc.	External authorities, received in both hard and soft copy.	Electronically on JDrive Hard copy originals held in cabinet.	Chief Executive, delegated management staff as needed	Digital files held in JDrive with restricted access Hard copies held in	Permanent – Do not destroy

Category	Source	Storage	Access	Security	Retention
				cabinet.	
Proof of course accreditation, registration, certification, etc.	External authorities, received in both hard and soft copy.	Electronic versions stored on JDrive Hard copy originals held in cabinet.	CEO, GGM and delegated staff as needed	Digital files held in JDrive t with restricted access Hard copies held in cabinet.	Permanent – Do not destroy

Schedule Normal Administrative Practice Guidelines

Normal administrative practice (NAP) is a process that allows the Institute to destroy certain types of low-value and short-term information in the normal course of business. It is an important tool to minimise costs of maintaining and managing records and data.

What can be destroyed under NAP?

Unofficial information and records of ephemeral value (i.e., records with little or no ongoing administrative, fiscal, legal, evidential or historical value) can be destroyed without authorisation as part of NAP when they are no longer needed for administrative, legal or other operational purposes.

Important: Institute records may only be considered for destruction under NAP when they are not covered – and don't need to be covered – by the Institute Records Retention and Disposal Authority (RDA).

Examples of information that may be destroyed under NAP:

NAP Type	Examples	Exclusions
Unofficial information	• Unsolicited emails (spam), or letters offering goods or services. • Unofficial personal email unrelated to work activities • Emails about going for coffee or lunch • Sites or folders with pictures of staff on holidays or their pets.	Emails about official work events.
Reference or duplicate copies	• Copies of records which are originated and already held within an Institute endorsed system, such as: Bigfoot, AMS and ELO. • Non-master copies of policies, procedures, reports, meeting material and communications. • Carbon copies (Cc) or blind carbon copies (Bcc) kept for convenience. • Copies of data used for reference or testing. • Decommissioned websites that have already been captured by the Institute's Web Archiving Program.	• Records where master copies no longer exist. • Digitised source records. • Backup copies of records and information used for the purpose of system recovery.
Rough working papers and calculations	• Routine or rough calculations working papers or background notes used to	Rough working papers and calculations containing significant decisions and/or

NAP Type	Examples	Exclusions
	develop drafts. • Spreadsheets or documents that have been incorporated into correspondence or a separate final document. • 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.	other significant information that is not contained in the final form of document.
Drafts not intended for further use	Draft documents which: • do not contain significant or substantial changes or annotations • are not required to document business activities.	Drafts formally circulated internally or released externally for review, comment and consultation and/or which incorporate substantial input that provides insight into the evolution of the final version, such as: • Draft policies, guides, industry rules etc. released for consultation. • Draft of high-level plans, strategies or reports released for consultation. • Draft agreements incorporating legal advice, which form part of contractual negotiations.
Transitory or short-term items	• Informal communications that do not support or contribute to administrative or operational functions. • Emails relating to system alerts, bounce backs, reminders. • Invitations, calendars and appointment diaries used for routine day-to-day operations and activities. • Zero byte files and empty folders.	Diaries used to record important matters or belonging to senior executives.
Publications produced by an external party	• Promotional or advertising material. • External publications and catalogues.	External promotional material that support and validate purchase decisions.

MELBOURNE
INSTITUTE OF TECHNOLOGY

Schedule x: File Naming Conventions Guidelines

Naming documents in a standardised, logical and intuitive way ensures that team members and collaborators can discover, manage and access Institute records when needed.

Why use naming conventions?

Using consistent naming conventions has many benefits, including:

- Improved retrieval of documents on shared drives and Institute systems
- Facilitated disposal of documents when no longer required for business
- Ensured current or active version of a templates can be easily identified
- Supported sharing of information within your team and with collaborators
- Easier and more efficient file naming for colleagues as they don't have to 're-think' the process each time.

Is there an Institute wide naming convention that my team can use?

No. Given the size and diversity of activities conducted by the Institute, having one single naming convention is not practicable. Instead, we recommend staff use the suggestions on this page to form guidelines that are useful and pragmatic for your School or department area.

What is an example of a good naming convention for folders and documents?

Good naming examples include:

- Academic Board/2025/25.1/Agenda/AB 25.1 Agenda
- BB101 Business Communications UD T1 2025
- BN208 Networked Application Assessment 1 T12025

How to develop naming conventions?

Establish good foundations

- Keep file names short but meaningful
- Include any unique identifiers, e.g. case number, project title, Student ID
- Be consistent
- Indicate version number where appropriate
- Ensure the purpose of the document is quickly and easily identifiable

Try to avoid

- Common words such as 'draft', 'letter', 'current' or 'active'
- Unclear, vague or repetitive e-mail correspondence titles
- Symbol characters such as: \ / < > | " ? [ ] ; = + & $ α β
- Abbreviations that are not commonly understood, or which may frequently change throughout time

Consult and identify needs

Discuss the naming conventions with your team and collaborators. For example:

- How does your team search for information?
- Is there anything specific that should be included?
- What key information is required to quickly and easily identify what a file or document is?

A unit may use internal identifiers for a project such as REC/Meeting 25.2/Student ID # Ethics Proposal

Document and review

Ensuring naming conventions are documented and made accessible to current and future staff, and included in local staff on-boarding process, will encourage staff to use them.

Reviewing the conventions each calendar year will ensure they remain current and relevant.