

Records Management Procedure

1. Purpose and Scope

- 1.1 The purpose of the Records Management Procedure is to operationalise the Records Management Policy.
- 1.2 This procedure applies to all AIAT business including governance, operational and academic activities. It concerns records which are created, collected, processed, used, archived, stored and disposed of in the conduct of AIAT business.
- 1.3 The procedure applies to all AIAT employees, independent consultants and contractors and other authorised personnel offered access to AIAT resources.
- 1.4 This procedure applies to all AIAT records management systems.

2. Definition

Refer to *Glossary of Terms*.

3. Procedure

- 3.1 Record Identification
 - 3.1.1 All AIAT records should be created and/or captured in a timely and efficient fashion.
 - 3.1.2 All managers and process owners are responsible for identifying what records need to be created or captured within their area of responsibility to establish a full and accurate account of AIAT's business activities and decisions. Examples of AIAT records can include, but are not limited to:
 - a. records of formal decisions taken by staff under delegation;
 - b. official communications to or from students, external persons and other organisations;
 - c. all correspondence created or received in the course of an investigation (eg misconduct, complaint, etc);
 - d. meeting papers of formally established AIAT boards and committees (including agendas, agenda papers, minutes, and reports);
 - e. meeting papers of ad hoc committees and working parties (including agendas, agenda papers, minutes, and reports);
 - f. contracts, agreements or legal documents;
 - g. financial transactions held electronically or in hard copy format;
 - h. personnel transactions (eg reports on performance and other dealings between staff and the AIAT);
 - i. subject outlines;
 - j. approved course and subject proposals and course accreditation documentation.

- 3.1.3 Staff should consider the purposes of AIAT records to evidence AIAT's business activities when determining whether a written note of a conversation should be made. A conversation only becomes an AIAT record when a written note (in any form) has been made of that conversation.
 - 3.1.4 To preserve the integrity of AIAT's records, no additions or alteration should be made to an existing record. If additions or alterations are required, a subsequent record should be created and added using consistent naming conventions.
- 3.2 Digital records
- 3.2.1 AIAT conducts its business as "digital by default", which results in digital source records. These should be captured, managed, used and retained in their original digital format wherever possible.
 - a. Conversion to another digital format should only be undertaken after consideration of the records management requirements, and any conversion between digital formats that results in a loss of context or degradation of the record (such as converting an email message to a PDF file) should be avoided.
 - b. The conversion of digital source records to a paper format (eg. print-outs for inclusion in a paper file) is not permitted, except where such records are required for further business action or for legal purposes.
 - 3.2.2 Naming of digital records
 - a. The naming of digital records assists in the ability to find, access and preserve these records. AIAT has adopted general naming conventions for its digital records (refer to Appendix B).
 - b. All digital records, irrespective of their source and format, are to be assigned a meaningful and consistent title at the time they are captured, consistent with the relevant naming conventions.
 - c. All managers and process owners, in consultation with the Director, Quality Assurance and Risk Management, are responsible for developing and documenting specific naming conventions for records within their area of responsibility.
- 3.3 Records Storage
- 3.3.1 AIAT uses and maintains records in a variety of corporate information systems. Refer to Appendix A for a list of approved corporate information systems.
 - 3.3.2 Digital records must be captured and managed within an approved corporate information system.
 - 3.3.3 Records that are created by an approved corporate information system should be stored in that system.
 - 3.3.4 Records that are not created and / or stored in an approved information system must be stored in the Electronic Documents and Records Management System (EDRMS). This includes but is not limited to email correspondence, word, excel and PowerPoint documents, video, audio, social media posts and telephone conversations (through recordings or file notes).

- 3.3.5 Consideration of records management requirements should be included during the development and implementation of corporate information systems and the associated business processes, and any subsequent changes to those systems and processes.
 - 3.3.6 Staff must not store records on network drives, laptops, temporary storage devices, portable drives, CDs, DVDs as these do not comply with recordkeeping requirements.
- 3.4 Use and management of records
- 3.4.1 Staff are to only access those files and records which are necessary for the proper fulfillment of their duties, or that they are lawfully requested to access.
 - 3.4.2 Under no circumstances are records to be accessed or used for non-institute related business.
 - 3.4.3 Personal information held on corporate information systems must only be used for the purpose with which it was collected and must only be disclosed to authorised persons.
 - 3.4.4 Staff leaving AIAT or moving roles within AIAT are responsible for ensuring records in their custody are made available to authorised staff.
 - 3.4.5 The access, use and disclosure of AIAT information and access to corporate information systems is subject to the requirements of the Privacy Policy, Staff Code of Conduct, and Information Technology Policy.
- 3.5 Disposal of records
- 3.5.1 Decisions on how long records are retained is based on the recordkeeping requirements of the record and detailed in the Retention and Disposal of Records Schedule (see Appendix C).
 - 3.5.2 AIAT records cannot be disposed of if:
 - a. they are identified as having historical significance and / or are classed as a permanent record;
 - b. they have not met the minimum retention timeframe as specified in Retention and Disposal of Records Schedule;
 - c. it is known that the records may likely be required in evidence, either now or in the future;
 - d. there has been an embargo placed on the disposal of records by AIAT or an external party;
 - e. it is identified that there is still a business requirement for the records to be retained.
 - 3.5.3 The Director Quality Assurance and Risk Management will annually review the Retention and Disposal of Records Schedule. A report outlining the records for disposal will be presented to the CEO for approval prior to actioning.
 - 3.5.4 Destruction methods used must ensure the confidentiality of records at all times from point of collection to final destruction and destruction methods must be irreversible. Destruction methods should be environmentally friendly where possible. The burning, burying or disposal of records at a landfill site are not

permitted. The destruction of records must be completed by an authorised contractor using authorised methods of destruction.

3.6 Breaches

- 3.6.1 Security and access to corporate information systems will be monitored and breaches reported to the CEO.
- 3.6.2 Not creating records at all, creating incomplete or inaccurate records, falsification and unauthorized modification may result in a breach of this policy and procedure.
- 3.6.3 Breaches under this policy and procedure will be managed under the Staff Code of Conduct.

4. Roles and responsibilities

- 4.1 The CEO is responsible for
 - 4.1.1 policy enforcement and compliance;
 - 4.1.2 general oversight of records, information and privacy management at AIAT;
 - 4.1.3 oversight of the AIAT records management system; and
 - 4.1.4 approving destruction of records.
- 4.2 The Director, Quality Assurance and Risk Management is responsible for
 - 4.2.1 the implementation and ongoing review of compliant records management system; and
 - 4.2.2 coordinating the destruction of records.
- 4.3 All staff are responsible for creating, capturing, using, and retaining AIAT business activity information and decisions in accordance with this policy and procedure.
- 4.4 All managers and process owners are responsible for
 - 4.4.1 identifying what records need to be created or captured within their area of responsibility; and
 - 4.4.2 documenting and implementing processes that ensure the correct management of AIAT records within their area.
- 4.5 All managers are responsible for the implementation of, and adherence to, this policy within their area of responsibility.

5. Procedure Details

Institution	Australian Institute of Advanced Technologies (AIAT)
Procedure name	Records Management Procedure
Procedure Reference No.	PROC – 46
Procedure Approval	Board of Directors
Procedure Authority	Executive Management Group
Responsible Officer	CEO
Governance Reference	6.1.3.e, 7.3.3.c

Threshold Standards	
Related Documents	<p>Acceptable use of ICT Policy</p> <p>Course and Subject Lifecycle: Proposal and Development Policy</p> <p>Course and Subject Lifecycle: Review, Monitoring and Change Policy</p> <p>Information and Communications Technology Policy</p> <p>Intellectual Property Policy</p> <p>Policy Framework Policy</p> <p>Privacy Policy</p> <p>Quality Assurance and Enhancement Policy</p> <p>Records Management Procedure</p> <p>Risk Management Policy</p> <p>Staff Code of Conduct</p> <p>Student Communication Policy</p>
Related Legislation	AS ISO 15489 Australian Standard Records Management
References	<p>AIAT has referred and benchmarked with the following institutions and policies during the creation of this procedure:</p> <p>Adelaide University (unknown) Information Management Procedure Manual, <i>retrieved 29 Sept 2021</i></p> <p>Australian Institute of Business (2022) Records Management Procedure</p> <p>Central Queensland University (2020) Records Management Policy and Procedure</p> <p>Curtin University (2018) Records and Information Management Procedures</p> <p>Kaplan (2020) Student Record Management Policy</p> <p>University of New England (2017) Records Management Procedures</p> <p>University of South Australia (unknown) Records Management Policy, <i>retrieved 29 Sept 2021</i></p> <p>University of Wollongong (2020) Records Management Policy</p>
Date of approval	2 December 2021
Review date	December 2026
Policy Category	Operational

6. Document Version Control

Document No	PROC - 46	Last Modify Date	Summary of Changes
Version No	1.0	NA	Initial version approved by Board of Directors
	1.01	31/3/2022	Fixed typos; update policy number; updated Appendix C

Created Date	Dec 2021		
--------------	----------	--	--

Appendix A: Corporate Information Systems

System	Record Types
	Personnel records
	Financial records
	Learning and teaching reports
	Work integrated learning records
	Student records
	Customer relationship records
	Information technology management and maintenance records
	Electronic Documents and Records Management System: Student records, personnel records, agreements and contractual records, administrative records, corporate records
	Property/facility management and maintenance records

Appendix B - AIAT E-File Naming Conventions and Version Control

A. Purpose and Scope

- A.1 The volume of digital records captured and managed by AIAT will increase as most of its business is conducted electronically. The ability to find, access and preserve these records depends largely upon where they are saved and how they are named.
- A.2 These conventions seek to ensure consistency in the naming of AIAT's electronic records, to facilitate the access, use and preservation of those records throughout the entire information lifecycle. Naming records according to these conventions will ensure record titles are consistent, logical and predictable.
- A.3 Meeting this standard will assist AIAT in meeting its compliance obligations, more effectively manage the electronic documents and records and provide for more consistent description of files, folders, documents and records. Consistent description leads to better availability, retrieval, integrity, accessibility and in some cases confidentiality.
- A.4 This appendix is relevant to all documents created by AIAT including, but not limited to, policies, procedures, charters, guidelines, plans, meeting minutes and agendas, and course and subject content.

B. General Rules

B.1 Version Control

- B.1.1 Version numbers are expressed as VXX.YY (for example V01.05).
- B.1.2 Modification to "XX" occurs when major changes are made to the document. The Approval Body must approve the updated version prior to use by the organisation.
- B.1.3 Modification to "YY" occurs when minor changes are made to the document. These changes are approved by the Responsible Officer.

B.2 File Name Structure

- B.2.1 The file name consists of the following elements:
 - a. Purpose of record, for example Policy or Procedure, Meeting minutes, charter, etc
 - b. Version number
 - c. Date

Examples:

Record Management Policy Draft V01.0 YYYYMMDD

Assessment Procedure V01.0 YYYYMMDD

Board of Director Minutes 22 July 2021 V01.0 YYYYMMDD

- B.2.2 If this model is not appropriate and no precedents are available, order the elements in a file name in the most appropriate way to retrieve the record. The elements to be included in a file name should be ordered according to the way in

which the record will be retrieved. For example, if the records are retrieved according to their date, the date element should appear first. If the records are retrieved according to their description, the description element should appear first.

- B.2.3 Use capital letters and spaces to delimit words. Eg Governance Charter V05.0 20210716.
- B.2.4 The version number in a file name is a two-digit number to assist with retrieving the latest version.
- B.2.5 For draft/in progress documents, use 'Draft' together with a version number, unless naming agendas/minutes.
- B.2.6 Versions apply to draft documents.
- B.2.7 The date in the file name must be 'back to front' and in this format: YYYY or YYYYMM or YYYYMMDD. Giving the dates back to front means that the chronological order of the records is maintained when the file names are listed in the file directory. This helps when trying to retrieve the latest dated record.
- B.2.8 When drafts or final versions are edited, the file must be resaved to the folder with new version number and, if applicable, new date.
- B.2.9 Once approved with no further immediate amendments the document is saved as a version 01 with approval date.
- B.2.10 Avoid creating file names containing these characters * : \ / < > | " ? [] ; = + & £ \$. You may encounter difficulties searching for or opening them.
- B.2.11 Note version and date only with no punctuation eg name of document V01.0 20210716
- B.2.12 The original author creates a document name with Draft V01. Each major edit and/or response by another author amends the document name to the following version number.

B.3 Naming files

- B.3.1 AIAT must not be in the title.
- B.3.2 The file name should reflect the purpose of the file, for example Policy or Procedure, Meeting minutes, charter.
- B.3.3 Avoid using acronyms and abbreviations wherever possible. Abbreviations may not be used consistently by or have the same meaning for all users. Acronyms may change over the course of an organisation's history, may have more than one meaning, or may related to more than one entity.
- B.3.4 Do not abbreviate words (such as 'DEPT' for Department, 'Jan' for January, 'mtg' for meeting, 'conf' for conference, etc) except where approved in these naming conventions.
- B.3.5 Do not use acronyms except in conjunction with the full name (e.g. "Academic Board (AB)").
- B.3.6 Where an acronym is used, do not separate the letters with full stops (e.g. C.S.I.R.O).

C. Storing

- C.1 Use meaningful folder names which indicate contents and activities.
- C.2 Establish folders for each committee, course and policy.
- C.3 Use Archive folders for each main folder. When documents have been finalised, all previous versions should be moved to the Archive folder.

D. Editing files

- D.1 Track changes should be used when reviewing.
- D.2 The original author must respond to any comments and is responsible for removing all comments once they are resolved.
- D.3 Each major edit and/or response by another author requires amendment of document name to the following version number as per the guidance in subsection B.1 above.

E. Policies, procedures and plans processes

- E.1 Documents are written by the author and reviewed by the responder. Policy Framework Policy guides key decisions.
- E.2 Where appropriate, organisational charts and diagrams can be included in the body of the documents.
- E.3 Key terms and definitions for each policy document are recorded on a central glossary document. Definitions will be suggested by the author, and reviewed by the responder. They will be alphabetically organised.
- E.4 Once the document is ready for Board review, all author and responder comments and track changes should be rectified and removed (to ensure a clean copy), and the date amended to the date it is sent to the appropriate Board.
- E.5 The document will be loaded in the appropriate Board's Policies and Procedures folder and Board Secretary will notify members that it is ready for review.
- E.6 After the Board minutes are released, documents are amended in terms of the Board feedback and, if appropriate, renamed as final version and recorded on the Policies and Procedures register.

F. Course and Subject content

- F.1 Documents are written by the author and reviewed by the responder.
- F.2 Once the document is ready for Course Development Committee (CDC) review, all author and responder comments and track changes should be rectified and removed (to ensure a clean copy), and the date amended to the date it is sent to the CDC.
- F.3 The document will be loaded in the CDC Course Review folder and CDC Secretary will notify members that it is ready for review.
- F.4 After the CDC minutes are released, documents are amended in terms of the CDC feedback and, if appropriate, renamed as final version.

Appendix C – Retention and Disposal of Records Schedule

Category	Minimum Retention Period
Corporate Tax Records <ul style="list-style-type: none"> • Income • Expenses • Liabilities • Assets (receipts, sales, purchases, etc) 	5 years (min) from the end of the accounting period. Longer if tax returns are late.
GST Records <ul style="list-style-type: none"> • Taxable supply • Importation • Creditable acquisition & importation 	5 years following the assessment period
Company Documents	
<ul style="list-style-type: none"> • Statutory books • Board minutes • Resolutions 	Permanent
<ul style="list-style-type: none"> • Accounting records with regards to transactions and all supporting documentation 	7 years
<ul style="list-style-type: none"> • Other business registers 	5 years (min) from date of last entry
Personnel Files (HR documents) <ul style="list-style-type: none"> • Employee records, payroll, wages, worker's comp, etc. 	7 years from EOFY
Student Records	
<ul style="list-style-type: none"> • Records of all students, including <ul style="list-style-type: none"> ○ name ○ current resident status ○ mobile phone number (if any) ○ email address (if any) ○ amount of money paid to AIAT ○ amounts owing to AIAT ○ duration of course paid for ○ written agreement(s) between the student and AIAT ○ up-to-date records of assessment 	Until two years after the person ceases to be a student
<ul style="list-style-type: none"> • Student financial records including <ul style="list-style-type: none"> ○ the total amount of fees ○ payment terms ○ any non-refundable deposit or administration fee ○ fees and charges for additional services 	7 years
<ul style="list-style-type: none"> • Student complaints and appeals records 	Five years from the date of the complaint or appeal was lodged
<ul style="list-style-type: none"> • Records required for legal action 	Retained until the completion of that legal action, including appeals

<ul style="list-style-type: none"> • Certification documentation, including: <ul style="list-style-type: none"> ○ A testamur and ○ Records of results, academic transcript or similar documentation. 	<p>Indefinite – electronic records containing information on student results for Australian Qualifications Framework (AQF) qualifications will be retained for 30 years after the student’s course completion date, to enable re-issuance of statements of attainment or qualifications (if required)</p>
<ul style="list-style-type: none"> • Examinations and assessments, including RPL assessment evidence 	<p>12 months from the date on which the grade decision was made (unless relating to a complaint or appeal – see above)</p>