RECORDS MANAGEMENT PROCEDURE

Approving Authority	General Manager	**Approval Date of Last Revision**	24 Mar 2022
Approval Date	23 Feb 2018	**Effective Date of Last Revision**	24 Mar 2022
Effective Date	23 Feb 2018	**Review Date***	28 Feb 2025
Document No	PRO8.1	**Version**	1.2
Parent Policy	Records Management Policy		
Policy Category	Operational		
Governing Authority	General Manager		
Responsible Officer	Executive Officer – Risk Management and Policy		
Related Documents	Records Management Policy ICT Policy and Procedure Risk Management Policy and Procedure Document Version Control Document Control Register Privacy Policy and Procedure Business Continuity Plan Higher Education Standards Framework (Threshold Standards) 2021 Education Services for Overseas Students (ESOS) Act 2000		

** Unless otherwise indicated, this Procedure will still apply beyond the review date.*

Contents

1. PURPOSE

1.1 The Records Management Procedure sets out the mandatory procedures for the implementation of Records Management Policy at Adelaide Institute of Higher Education (AIHE).

2. SCOPE

2.1 The Records Management Procedure applies to all AIHE's staff, contractors and consultants, all aspects of AIHE's operations, all records created or received in any format to support AIHE business activities and all business applications used to create, manage and access records.

3. RECORDS MANAGEMENT APPROACH

3.1 AIHE will meet its recordkeeping compliance obligations through:

- establishing recordkeeping as a systematic part of its business operations so that records are identified, captured, managed and retained in an accessible, confidential and usable format that preserves the integrity of those records over time;
- deployment of the Institute's Document's Register as the primary driver for records management compliance at AIHE;
- management of an AIHE's Version Control; and
- provision of appropriate training, support and documented procedures for AIHE personnel.

4. RECORDS MANAGEMENT SYSTEMS

4.1 AIHE maintains a number of approved electronic systems for the purpose of recordkeeping:

- Xero (Budget and Finance);
- Meshed (Student Records);
- Canvas (Learning Management System); and
- AIHE's Document Register (Corporate, HR, Student/Faculty/Units) at server of AIHE.

In addition, there may be a number of other electronic, paper-based, micrographic and audio-visual systems which have some form of limited recordkeeping functionality and capability.

4.2 It is mandatory for all AIHE's records (final version) to be recorded in its approved records management systems, as follows:

- all staff to ensure AIHE's records are recorded, managed and disposed of using the AIHE records management systems; and
- all records contained in the records management systems shall be securely stored and used in accordance with ICT Policy and Procedure.

5. RECORDS CREATION

5.1 All staff are required to create full and accurate records which adequately document the business activities in which they take part.

5.2 Records should be full and accurate to the extent necessary to:

(i) facilitate action by employees, at any level, and by their successors;

(ii) make possible a proper scrutiny of the conduct of businesses by anyone authorised to undertake such scrutiny;

(iii) protect the financial, legal and other rights of the organisation, its clients and any other people affected by its actions and decisions.

6. CONTROL OF RECORDS

6.1 Version control

6.1.1 Earlier versions (i.e. drafts) of a document may be deleted once the previous versions are no longer needed to create future records. However, drafts that must not be disposed of are those that document significant decisions, reasons and actions and contain significant information that is not contained in the final form of the record. This applies to both paper and electronic drafts.

6.1.2 The final version of a document will be saved in pdf format.

6.2 Security and confidentiality

6.2.1 Records must be made accessible to authorised users. Staff of the Institute enacting the normal course of their duties must have access to relevant records of the Institute.

6.2.2 Personal information about staff and students of AIHE must be secured confidentially within all levels of AIHE records. [For further details on handling personal information refer to the AIHE Privacy Policy.]

6.3 Storage

6.3.1 Records should be stored in conditions that are clean and secure, with low risk of damage from fire, water, dampness, mould, insects and rodents. They should also be kept away from direct sunlight and other sources of light and heat. The storage area should be well ventilated and ideally maintained at a stable temperature and humidity.

6.3.2 Records in non-paper formats such as photographs, maps or computer disks require specialised storage conditions and handling process that take account of their specific physical and chemical properties. Irrespective of format, records of continuing value require higher quality storage and handling to preserve them for as long as that value exists.

6.3.3 All stakeholder hardcopy files will be kept in a secure fashion i.e. lockable filing cabinet. All electronic records will be kept in pass word protected directories with access limited to a ‘need basis’.

6.4 Access to records

6.4.1 Staff, contractors, consultants and other third parties may, subject to appropriate authority, have access to AIHE records to fulfil their duties and obligations.

6.4.2 It is the expectation of the Institute that a staff member will access only those files and records that are necessary for the performance of duties of the position to which they are appointed, or, that they are lawfully requested to access.

6.4.3 All staff with access to AIHE’s approved records management system will have signed a Confidentiality Agreement at the commencement of their employment.

6.4.4 All stakeholders will be permitted access to their personal information by applying in writing and having given 5 working days - notice. A small administrative fee may apply for retrieval from archive or for copies. Identification will need to be provided prior to handover of personal information.

6.4.5 Under this policy the Institute reserves the right to access any AIHE business record, created or received by staff, irrespective of its format or storage location.

6.5 Information privacy

6.5.1 In accordance with the principles of the *Information Privacy Act 2009*, AIHE will take appropriate measures to ensure the security of personal information and records to protect it against loss, unauthorised access, use, modification or disclosure, and against any other misuse.

6.5.2 Under existing administrative access arrangements staff and students are able to access their own staff or student file.

6.6 Right to access personal information

6.6.1 Persons may obtain access to documents concerning their personal affairs held by AIHE, and seek amendment of information held by AIHE concerning their personal affairs if that information is inaccurate or incomplete.

6.6.2 Access to certain documents or to certain information contained in documents may be refused to protect essential private or business affairs of others.

6.6.3 The person's right of access is not affected by any reason the person gives for seeking access.

7 RETENTION, DISPOSAL AND DESTRUCTION OF RECORDS

7.1 A Records Retention Schedule will be developed for corporate and academic records.

7.2 Retention of student records

The schedule below details requirements for the retention of student records.

The ‘retention period’ is from a student’s graduation date or the date at which an international student ceases to be an accepted student.

#	Documents	Examples of documents	Retention period*
1	Admission files	Enrolment Application Letter of Offer Acceptance of Offer Letter Application for Credit Form Student personal information, identification and contact	6 years
2	Student files	Student ID Payment document Warning letter on the progression toward the degree Dismissal Transferral Examination results Assessment/assignment results	6 years for assessment results. 1 year for submissions that are hard-copy and not assignment, assessment or examination results.
3	Record of critical incident involving a student and remedial action taken by AIHE	Critical incident report form	At least 2 years
4	Transcripts, Certification of Enrolment and Degrees		30 years

* The **'retention period'** is from a student's graduation date or the date at which an international student ceases to be an accepted student, whichever is longer.

7.3 Retention of organisational corporate documents

The schedule below details requirements for the retention of organisational corporate documents.

#	Documents	Examples of documents	Retention period
1	Training agreement/contract with a third party private or public organisation		7 years from the agreement/contract termination
2	Financial records	Financial Annual Report Invoices	7 years from the date of the report
3	Employment related documents	Employee personal information Employment contract Payment information	7 years from the employment contract termination
4	Operational health and safety records		7 years 27 years for those that relate to persons with mental health illnesses
5	Corporate document retention as required by ATO	Refer to https://www.ato.gov.au/Super/Self-managed-super-funds/Administering-and-reporting/Record-keeping-requirements/	5 – 10 years

7.4 Disposal of records

7.4.1 Any document that contains non-public information about students or applicants and employees — especially sensitive items such as admission applications, letters of recommendation, grades, or private contacts and addresses — should receive special handling when retention is no longer needed. It should either be shredded or destroyed in some way that maintains its confidentiality.

7.4.2 When records are due for disposal they will be securely destroyed through the use of an approved confidential bin provider by authorised staff in each operational unit where they were created. Secure document destruction bins are available on campus.

8. ARCHIVING AND BACKUP

8.1 Archiving – Where files require archiving, they will be adequately protected, boxed and recorded prior to removal from AIHE's premises. Archive records will be kept electronically.

8.2 Backup – All electronic data at AIHE's Information Management and Record Keeping system will be backed up on a daily basis to external hard drives and to a Cloud for offsite storage.

8.3 Records transfer – In the event that AIHE ceases operation, the Risk Management Policy and Plan in the case of operational cease will become operational. Records Transfer will be made to a third party.

8.4 Audit and review – This Procedure is reviewed on biennial basis to accommodate changes in legislation, technologies, programs and resources available to the Institute.

9. DEFINITIONS

9.1 See the AIHE Glossary of Terms for definitions.

Document Control

Version #	Date	Key changes
1.0	23/02/2018	Procedure approved by General Manager
1.1	27/03/2019	Addition of retention period for international students at 7.2
1.2	24/03/2022	Updated the procedure's Responsible Officer to Executive Officer Risk Management and Policy, Updated names of AIHE records management systems in Sec 3&4, updated reference to 2021 HES Framework.