Records and Data Management Policy and Procedure

Purpose

1. The Australian International Institute of Higher Education ('the Institute') recognises that the preservation and management of records pertaining to the full range of institutional activity is critical to effective business operations, transparency, and accountability in relation to decisions taken at the Institute.
2. This Policy provides guidance to the staff of the Institute in relation to the creation, management, storage, retrieval, and disposal of records. This Policy complies with relevant legislative and regulatory standards as well as good practice principles in business records management.

Scope

3. This Policy applies to:
   a) all staff of the Institute whether full-time, part-time, casual or contract
   b) members of the Institute's Governing Bodies
   c) individuals engaged in providing services to the Institute or receiving services from the Institute, such as students, contractors or consultants
   d) all records generated within the Institute including paper-based and electronic records and all data.

Definitions

4. For the purposes of this Policy:
   a) ***Business records:*** means records in paper-based or electronic format that capture the everyday activities of the Institute including qualitative and quantitative data.
   b) ***Data:*** means facts and statistics collected together for reference or analysis.
   c) ***Electronic records:*** means any records captured by any technological means that are secured through daily, automatic backup.
   d) ***Marketing records:*** means documents in paper-based or electronic format that promote the Institute and the courses offered and include website content, a handbook for students and marketing brochures.
   e) ***Non-essential records:*** means records that have expired their legislated preservation period and are not deemed essential to the ongoing operation of the Institute.
   f) ***Privacy Act 1988***: is the Australian law that regulates the handling of personal information about individuals. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. The *Privacy Act* includes thirteen (13) Australian Privacy Principles (APPs). The APPs set out standards, rights, and obligations for the handling, holding, use, accessing and correction of personal information (including sensitive information).

g) ***Records:*** means any information captured by hard copy, technological or electronic means that pertains to the Institute and its community.

h) ***Staff records:*** means any record relating to individual staff.

i) ***Student records:*** means records in paper-based or electronic format that capture data pertaining to the student journey including records of application, enrolment, academic progress, departmental interactions, and graduation.

Policy

Principles

Records

5. The Institute recognises that it generates important and extensive records related to teaching, scholarship, students, staff, finances, business administration and other activities and is committed to good practice in the creation, management, retrieval, security, and disposal of such records by this Policy.
6. Personal privacy and risk mitigation are fundamental considerations in the management of all corporate and personal records.
7. Access to all records is restricted to authorised staff with a business process requirement.
8. Record management training will be undertaken as part of all staff induction.

Data

9. Data is collected only for the following purposes:
   a) to support the Institute's operational activities
   b) to inform quality improvement, risk management and strategic planning
   c) to meet external reporting requirements.
10. Collection of accurate and complete data is the responsibility of all Institute staff.
11. Personal data held by the Institute is collected and managed in a responsible manner.
12. Data is protected from unauthorised access and modification, and disposal of data is undertaken securely on the basis of approved applications.
13. Data is only made available to third parties in accordance with legal and regulatory requirements.

Procedure

General requirements

Record creation and capture

14. All staff are required to maintain accurate records of all activity for which the Institute may be held accountable and integrate these records within the Institute's records management system in compliance with this Policy. All documents must be marked with version control including the date of record creation/update.

Record storage, archiving and disposal

15. In determining appropriate storage for current and non-current records, consideration must be given to the protection provided by any selected storage facility, sensitivity of records, required retention periods as well as access requirements and demands.
16. Staff are responsible for applying adequate security measures for the access and use of records in accordance with legislative, regulatory or business requirements. Records should be accessible on a 'need-to-know' basis and security arrangements should provide for reasonable protection and detection of breaches.

    Staff must not relinquish, amend, destroy or damage records belonging to the Institute without approval from the Chief Executive Officer (CEO) in accordance with the *Authority Delegation Policy.*
17. Staff may destroy non-essential records after relevant legislated retention periods as below:
    a) business records must be kept for a minimum of seven (7) years
    b) student records must be kept for a period of two (2) years after the student's graduation, except for records necessary to re-issue or authenticate students' academic transcripts or testamurs, which must be kept in perpetuity
    c) staff records must be kept for a minimum of five (5) years after the staff member has ceased employment at the Institute.

Record security and data protection

18. The security of records is established through electronic back-up, and/or secure storage on-site or off-site in an area where records are protected from damage and incursion but may be retrieved as required and authorised. Measures for the prevention of unauthorised access, disclosure or alteration of personal, sensitive or otherwise confidential information include the following controls:
    a) the Student Services Manager may only provide access to student and staff records, respectively, on a 'need-to-know' basis
    b) third-party access to personal information is limited to what is permitted under the Institute's *Personal Information and Privacy Policy*
    c) physical records are stored in secured areas or secured cabinets
    d) contracts with external parties that may access or be provided with Institute records have relevant legal provisions included in their contracts, and are inducted, on the Institute's records management requirements and processes. Hiring managers are responsible for ensuring that contractors abide by the relevant contractual provisions and Institute policies.
19. The Institute has processes and controls in place for the protection of data. The Institute identifies critical data loss scenarios and implements controls accordingly. Security protocols implemented based on the classification of the data include:
    a) access control
    b) separation of duties
    c) least privilege
    d) session lock
    e) wireless access restrictions
    f) media protection
    g) software usage restrictions.

Record categories – specific requirements

Business records

20. Business records are recognised as records of everyday business activities conducted by and at the Institute which:
    a) facilitate the work of current and successive staff
    b) provide adequate access to information for authorised persons
    c) protect the rights of the Institute and its community.
21. These records include, but are not limited to:
    a) formal communications between staff of the Institute and internal and external bodies and departments
    b) formal communications between staff and students
    c) policy decisions and amendments including procedural changes
    d) negotiations with external parties on behalf of the Institute
    e) transactions conducted on behalf of the Institute with internal or external parties, including financial transactions
    f) precedential advice or activity
    g) any action or decision that may impact on the Institute's staff, students, clients, and/or associated organisations.

Marketing records

22. Marketing records promote the Institute, its facilities, staff and courses to prospective students. Information developed for this purpose is used for the website, the student handbook and brochures, and will be retained for two years.

Student records

23. The Institute recognises that it has a duty of care towards students and must therefore preserve and protect student information generated at the Institute in a manner that satisfies privacy laws, record management and retention regulations.
24. In accordance with the 'need-to-know' principle, student records are only accessible to the Academic Dean and staff from the Student Services and Admissions units.
25. The following are examples of appropriate records.

Student files

26. All students are allocated an individual file upon formal application for enrolment at the Institute. The student file must contain at a minimum:
    a) application and certification documentation, enrolment data, financial transactions (including receipts of student payments), academic results and progress information, formal communications between staff and students, and any incidents involving individual students such as:
        i. complaints
        ii. allegations of misconduct and breaches of academic integrity
        iii. critical incidents.

b) external communications about students that are generated by the Institute, including the Student's signed Written Agreement.

27. Student file records must be stored securely for a minimum period of two (2) years after the person ceases to be a student, whether as a result of withdrawal from an Institute course or when the person graduates.

Student data

28. Electronic records must be generated for each student across all enrolment periods.
29. The academic results of all students are to be kept in electronic, password-protected, secure formats for the period of student enrolment as well as two (2) further years after student graduation.
30. Student records required for transcript and/or testamur re-issue are categorised as perpetual records and must be retained by the Institute indefinitely.

Student Personal Details

31. The Institute is required to maintain accurate and up-to-date information on accepted students, including contact details, and provide this data to the Tertiary Education Quality and Standards Agency under certain circumstances.
32. The Institute requires students to ensure that their contact details are correct and up to date at all times:
    a) commencing and continuing students are required to confirm their personal details during the enrolment process for each study period as per the relevant *Enrolment Policy*
    b) students are regularly reminded to notify the Institute of any change to their contact details.

Staff records

33. All staff at the Institute are allocated a staff file from the point of employment. The staff file must contain at a minimum staff job application documents including certified qualifications, Curriculum Vitae, appointment details, awards, documentation in relation to any misconduct, police clearance documents or service contracts and performance reviews.
34. Electronic staff records must capture staff payments, taxation, superannuation and any associated financial activity between the Institute and staff.
35. In accordance with the 'need-to-know' principle, staff records are only accessible to the CEO, the Academic Dean (for academic staff), and the direct supervisor.
36. The Institute must keep copies of staff records available at the request of any staff or by a former staff member. Staff will have access to their records/files.

Responsibilities

37. Records management is the overall responsibility of the CEO and the Governing Council.
38. The Student Services Manager is responsible for the management of student records.
39. Managers are responsible for records management pertaining to their business area and their reporting staff.

Associated information

Approving body	Governing Council
Date approved	23 October 2020
Date of effect	Commencement of operation
Scheduled review	Two years from when policy commence
Current version approval date	15/08/2024
Next review date	15/08/2026
Policy owner	Chief Executive Officer
Policy contact	Chief Executive Officer
Related AIIHE Documents	Authority Delegation Policy Compliance Policy and Procedure Domestic Student Enrolment Policy and Procedure International Student Enrolment Policy and Procedure Personal Information and Privacy Policy and Procedure Quality Assurance Framework
Higher Education Standards Framework (Threshold Standards) 2021 (Cth)	Standard 7.3, ss 3
Other related external instruments/documents	**Related Legislation** • Tertiary Education Quality and Standards Agency Act 2011 (Cth) • Education Services for Overseas Students Act 2000 (Cth) • National Code of Practice for Providers of Education and Training to Overseas Students 2018 (Cth) • Privacy Act 1998 (Cth) • Corporations Act 2001 (Cth) • Evidence Act 1995 (Cth) • Electronic Transactions Act 2001 (Qld)

Document history

Version	Author	Changes	Approval Date
1.0	Not applicable	Original version	23 October 2020
1.1	Compliance Officer	Reviewed to align with the HESF 2021 and the footer was updated with current addresses.	15 August 2024

N.B. The document is uncontrolled when printed! The current version of this document is maintained on the AIIHE website at www.aiihe.edu.au.