ZENITH INNOVATION INSTITUTE
UNPARALLELED EXCELLENCE

Records and Data Management Policy and Procedure

Approving body	Governing Board (GB)
Date approved	27 Feb 2025
Date of effect	Commencement of operation
Next scheduled review	Two years from policy commencement
Policy owner	Chief Executive Officer
Policy contact	Chief Executive Officer
Related Documents	Delegations Policy and Schedule Student Enrolment and Completion Policy and Procedure Personal Information and Privacy Policy and Procedure ICT and Cyber Security Management Policy and Procedure
Higher Education Standards Framework (HESF) 2021 (Cth)	Standard 1.2 Standard 1.5.4 Standard 1.5.7 Standard 2.4.4 Standard 4.1.3 Standard 5.3.7 Standard 6.1.3e Standard 7.3.3

Purpose

1. **Zenith Innovation Institute** (**'Zenith / the Institute'**) recognises that the preservation and management of records pertaining to the full range of institutional activity is critical to effective operations, transparency, and accountability in relation to decisions taken at the Institute.

2. This Policy provides guidance to staff of the Institute in relation to the creation, management, storage, backup, retrieval, and disposal of records. This Policy complies with relevant legislative and regulatory standards as well as good practice principles in 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; and

(d) all records generated within the Institute including paper-based and electronic records and all data.

Policy

Principles

4. A full and accurate record of activities of the Institute will be created, captured and maintained in systems with appropriate recordkeeping functionality and controls.

5. Records will be made available within the constraints of security, confidentiality, privacy and archival access conditions.

Records

6. The Institute recognises that it generates important and extensive records related to teaching, learning, research 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.

7. Personal privacy and risk mitigation are fundamental considerations in the management of all corporate and personal records.

8. Access to records is restricted to authorised staff with a business process requirement.

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; and

   (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

14. This procedure outlines record keeping procedures and processes as follows:

   (a) General requirements for record keeping;

   (b) Specific requirements by record type; and

   (c) Staff records.

General requirements for record keeping

15. The general requirements for record keeping are outlined below and include:

    (a) Record creation and capture;

    (b) Record storage, archiving and disposal; and

    (c) Record security and data storage.

Record creation and capture

16. All members of staff are required to create, capture and appropriately manage records relating to their work, regardless of the format of the records and including records of decisions made and actions taken. Records will be maintained (stored and preserved) in conditions suitable to the length of time they need to be kept and made available for use. This applies regardless of the format of the records or the media they are stored on.

17. All documents must be marked with version control numbering and authority.

Record storage, archiving and disposal

18. 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.

19. Zenith will apply 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.

20. CEO approval is required prior to Institute being relinquished, amended, destroyed or damaged, noting that the following legislated retention periods apply:

    (a) business records must be kept for a minimum of seven (7) years;

    (b) marketing records must be kept for a minimum of two (2) years;

    (c) 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 testaments, which must be kept in perpetuity; and

    (d) 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

21. 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 and is governed by the Institute's *Personal Information and Privacy Policy and Procedure*;

    (c) physical records are stored in secured areas or secured cabinets; and

(d) contracts with external parties which 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.

22. 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 and primarily include access control and restrictions.

Specific requirements by record type

23. There are two record types have special and specific requirements that must be followed. These are outlined below and include:

(a) Student records; and

(b) Staff records.

Student records

24. 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.

25. In accordance with privacy principles, student records are only accessible to the Academic Dean and staff from the Student Services and Admissions units.

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, 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; and

(iv) external communications about students that are generated by the Institute.

27. Student file records must be stored securely for a minimum period of two (2) years after the graduation of the student.

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 (**TEQSA**) under certain circumstances.

32. The Institute requires students to maintain up-to-date and correct contact details 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*; and

    (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 at the point of employment. The staff file must contain at minimum staff job application documents, including: certified qualifications, resume, appointment details, awards, documentation in relation to any misconduct, police clearance documents or service contract 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, 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 Board (GB).

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.

Definitions

26. For the purposes of this Policy and Procedure:

Term	Definition
Business records	Business records are recognised as records of everyday business activities conducted by and at the Institute which: • facilitate the work of current and successive staff; • provide adequate access to information for authorised persons; and • protect the rights of the Institute and its community. Business records include, but are not limited to: • formal communications between staff of the Institute and internal and external bodies and departments; • formal communications between staff and students;

Term	Definition
	• policy decisions and amendments including procedural changes; • negotiations with external parties on behalf of the Institute; • transactions conducted on behalf of the Institute with internal or external parties, including financial transactions; • precedential advice or activity; and • any action or decision that may impact on the Institute's staff, students, clients, and/or associated organisations.
Data	Facts and statistics collected together for reference or analysis.
Electronic records	Any records captured by any technological means which are secured through daily, automatic back-up.
Marketing records	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.
Non-essential records	Records that have expired their legislated preservation period and are not deemed essential to the ongoing operation of the Institute.
Privacy Act 1988	The Australian law which 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).
Records	Any information captured by hard copy, technological or electronic means that pertains to the Institute and its community.
Staff records	Any record relating to individual staff.
Student records	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.

Version history

Version	Changes	Approval Body	Approval Date
1.0	New Policy	Governing Board	
1.1	Updated 20 c) from 5 years to 2 years	Governing Board	19 Sep 2024

Version	Changes	Approval Body	Approval Date
1.2	Updated related documents to reflect correct names	GB	27 Feb 2025