ZENITH INNOVATION INSTITUTE
UNPARALLELED EXCELLENCE

Personal Information and Privacy 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 (CEO)
Policy contact	Chief Executive Officer (CEO)
Related Documents	Delegations Policy and Schedule Quality Assurance Framework Records and Data Management Policy and Procedure ICT and Cyber Security Management Policy and Procedure
Higher Education Standards Framework (HESF) 2021 (Cth)	Standard 2.4.4 Standard 7.3.3 *National Code of Practice for Providers of Education and Training to Overseas Students 2018* (**National Code**). *Education Services for Overseas Students Act 2000 (ESOS Act)* *Privacy Management Framework*[1] of the Office of the Australian Information Commissioner for alignment with the *Australian Privacy Principles*

Purpose

1. **Zenith Innovation Institute** (**Zenith / the Institute**) recognises that privacy is a human right and has responsibilities and obligations when handling personal information.

2. This Policy provides an overview of the personal information held by the Institute, and personal information handling practices, procedures and systems. This Policy complies with relevant legislative and regulatory standards as well as good practice principles in the management of personal information

Scope

3. This Policy applies to:

   (a) members of the Institute's governing bodies;

[1] https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice, accessed 25.07.2022

(b) all prospective and enrolled students and alumni of the Institute;

(c) all staff of the Institute, whether full-time, part-time, casual or contract;

(d) all personal information held by the Institute regardless of format.

Policy

Statement

4. The Institute deals with personal, often sensitive, information about individuals and has a responsibility to preserve and protect personal information. The Institute is committed to good practice in when managing of personal information as outlined in this Policy.

Principles

5. When handling personal information, the Institute shall act in accordance with the *Privacy Management Framework*[2] of the Office of the Australian Information Commissioner for alignment with the *Australian Privacy Principles*[3] , and will:

(a) **Culture**: foster a culture of respect of privacy to reduce invasiveness as far as practicable.

(b) **Processes and Protections**:

(i) embed privacy protections into the design of information-handling practices;

(ii) maintain the quality of personal information that is used and disclosed;

(iii) only disclose student information with the consent of the student or only do so if the student would expect it, or where legally required to do so;

(iv) Staff members receive privacy training during induction and are aware of the potential adverse consequences of unnecessary invasiveness and of privacy breaches.

(c) **Continuous improvement**:

(i) regularly conduct activities to identify, assess and manage privacy and security risk, as well as develop and monitor controls for those risks;

(ii) regularly review its activities and consider whether it is necessary to collect and hold personal information in order to carry out the specific functions or activities.

Procedure

Purpose and type of information collected

6. The Institute collects information for a range of purposes. These purposes are largely focused on Zenith's primary purpose of delivery higher education courses, supporting and improving student support and meeting legislative or regulatory requirements.

7. The Institute collects personal information through a variety of methods, including online forms, direct interaction with individuals, security cameras, network use, or audio and video recordings of events.

8. The Institute will take steps to ensure that students and staff are appropriately notified where personal information is collected.

9. Personal information collected and a summary rationale is provided at Table 1.

Table 1 | Summary overview of information collected by the Institute

[2] https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice, accessed 25.07.2022

[3] https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference, accessed 25.07.2022

Purpose	Description/rationale	Type of information
Admission	To allow reasonable adjustments and disability support	Full name, date of birth, gender, contact details, billing address, tax file number, passport document number, bank account number, driver’s licence number, emergency contacts, details of next of kin.
Administration	To provide advice regarding access	Payment records.
Human resource (HR) management	Information regarding investigation into potential breaches of relevant codes of conduct and policies	Employment and related human resource records.
Staff Personal Information	Information regarding staff personal information and employment is only accessible to relevant personnel.	Full name, date of birth, gender, contact details, billing address, tax file number, passport document number, bank account number, driver’s licence number, emergency contacts, details of next of kin.
Safety and security	For example, non-anonymous surveys or feedback of the student or staff experience, educational offerings, curriculum, or support services	Recorded images.
Equal opportunity measures	To allow reasonable adjustments and disability support	For students, specific enrolment- and course-related information such as: • health and other personal information, e.g. as collected by Student Services or supervisors; • all applications, including admission, special consideration, reasonable adjustment, review of assessments.
Support services	To provide advice regarding access	
Grievance and appeals processes	Information regarding investigation into potential breaches of relevant codes of conduct and policies	• Breaches of codes of conduct or other policies, including sanctions and penalties • Information relating to grievances, complaints and appeals.
Quality improvement	For example, anonymous surveys or confidential feedback of the student or staff experience, educational offerings, curriculum, or support services	• Surveys, focus groups or other feedback mechanisms. • As far as possible, the Institute will use de-identified data and provide an option to remain anonymous where possible, e.g. when responding to surveys.
Graduation certification	As necessary for authentication purposes	• Variations to enrolment. • Assessment results, academic transcripts, testamur and attainment records.

Purpose	Description/rationale	Type of information
Alumni network	As required for the Alumni on an opt-in basis	• Contact details. • Course details •
Legislative or regulatory	As required to meet any legislative, regulatory or other legal obligations	• As required.

10. The Institute will provide an individual with access to their personal information when requested in writing or with proof of identity by the individual and if the identity of the individual has been established. An individual need not provide a reason for requesting access to their personal information.

11. The Institute takes reasonable steps to ensure that the personal information it holds is accurate, up-to-date, complete and relevant, and will correct personal information when requested by individuals in writing or with proof of identity, having regard to the purpose for which it was collected.

Storage and security

12. The Institute takes reasonable steps to protect personal information from misuse, interference, loss, and from unauthorised access, modification or disclosure.

13. The Institute implements strategies to eliminate or mitigate:

    (a) **human error risk** by raising awareness of staff members during induction, and providing regular updates;

    (b) **trusted insider risk** by monitoring access to systems hosting personal information and regularly reviewing audit logs, such as:

    (c) **access risk** by:

        (i) limiting access to personal information to those staff / students necessary to enable the Institute to carry out its functions;

        (ii) number of users with administrative privileges limited to staff / students requiring those privileges;

        (iii) physically disabling USB or other external port access to devices on devices of staff / students with access to sensitive information.

14. The Institute uses four main strategies to minimise human error risk, trusted insider risk and access risk are outlined at Table 2.

Table 2 | Information disclosure risk strategies

Strategy	Description
Risk assessment	The Institute conducts regular privacy impact assessments, information security risk assessments and reviews of personal information security controls in accordance with its *Risk Framework*. The Institute ensures that risk assessments are conducted following significant changes to organisational structure, technological systems, or legislative requirements.
Training and professional development	The Institute provides training and regular refreshers on physical and ICT security and the handling of personal information to permanent and casual staff and contractors. The training includes information on the importance of not accessing personal information or databases unnecessarily, what would constitute misuse of personal information, identity authentication procedures, and on recognising and avoiding inadvertent disclosures when

Strategy	Description
	for example verifying students' identity or publishing information on the Institute's website or Learning Management System.
Continuous review	Other security controls include: regular review of rights to access to personal information, revocation of such access when staff leave the organisation or change roles, protocols for the printing of documents containing personal information, the application of labels with the Institute's contact details on mobile devices in case of loss, and use of remote wiping software to allow for the deletion of personal information stored on devices which have been lost or stolen.
Systems measures	The Institute ensures the adequacy of security protections of its systems with its suppliers, including by ensuring the use of measures such as antivirus, firewall, continuous monitoring of servers for possible attacks, regular patches and updates, encryption of data, authentication of users, encryption of login details, and regular and multiple back-ups of data.

Disclosure by the Institute

15. The Institute will not disclose an individual's personal information to persons other than the individual unless:

    (a) the individual is reasonably likely to have been aware, or made aware that information of that kind is usually passed to that person or organisation;

    (b) the individual has given written consent to the disclosure;

    (c) the Institute believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual;

    (d) the disclosure is required or authorised by or under law or;

    (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

Government agencies, Third parties and overseas recipients

16. The Institute may disclose personal information to Australian Government agencies and relevant authorities, such as the Department of Home Affairs, Department of Education, Australian Tax Office, relevant Overseas Student Health Care Providers, federal and state law enforcement, or the Tuition Protection Service.

17. The Institute may disclose student personal information to third parties when reasonably necessary during a student's course, such as when applying to a Work Integrated Learning host organisation. In those instances, the Institute will ensure that only necessary personal information for the purpose of the placement is disclosed.

18. The Institute enters into agreements with third parties which include provisions to ensure compliance with privacy laws.

19. The Institute may disclose personal information to overseas recipients, especially in certain cases regarding international students. This may include verification of graduation.

20. The Institute will only provide this information as per the above disclosure principles, where it has established an agreement which would ensure compliance with Australian privacy laws, or where the Institute thinks the recipient is subject to laws which are substantially similar to the *Privacy Act 1988*.

Disposal

21. Personal records must be retained and disposed of or destroyed as outlined in the *Records and Data Management Policy and Procedure*.

22. The Institute will regularly review personal information it holds to determine if the information is needed.

Breaches of Australian Privacy Principles

23. The Institute is required to notify affected individuals and the Office of the Australian Information Commissioner in the event of ‘eligible data breaches’. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates. The Institute conducts a prompt and reasonable assessment if an eligible data breach is suspected.

24. Where a member of staff becomes aware of, or suspects, a data breach, the nominated Privacy Officer must be notified of this. The notification should include a description of the breach time and date of the incident or discovery of the breach, type of breach, type of information involved in the breach, likely cause of the breach, and any action taken to mitigate the impact of the breach. The Privacy Officer must keep a record of the notification and incident.

25. The Privacy Officer will assess whether the breach involves personal information and the severity of the breach, taking into account the sensitivity of the information, volume of data involved in the breach, and risk of harm to individuals.

26. The Privacy Officer will coordinate a response to the breach in consultation with the CEO. Depending on the extent of the breach, the Privacy Officer may form a response team, which will be composed of the Executive Management Committee members and other staff as required. The Privacy Officer will ensure that immediate remedial action takes place to contain the breach and prevent further breaches.

27. Where the incident is an eligible data breach, the Privacy Officer will notify the Office of the Australian Information Commissioner, including a description of the data breach, the kinds of information involved, and recommendations about the steps individuals should take in response to the data breach. The CEO will inform the Governing Board (GB) of the breach and the institutional response to the breach.

28. The Privacy Officer will notify the affected individuals, including outlining:

    (a) actions taken by the Institute to mitigate the breach and prevent further breaches;

    (b) steps that they can take to reduce the risk that they experience serious harm as a result of the breach;

    (c) that the Office of the Australian Information Commissioner has been notified of the matter (as applicable).

29. The Privacy Officer will review the incident, consider actions needed to prevent future breaches, discuss with the Executive Management Committee, and report on the matter to the Audit and Risk Committee and ultimately to the Governing Board (GB) with proposed improvements.

Complaints

30. Complaints relating to personal information may be addressed under the provisions of the *Student Grievance Policy and Procedure* or the *Human Resources Management Policy and Procedure*.

Responsibilities

31. Personal information is the overall responsibility of the CEO and the Governing Board (GB).

32. The Student Services Manager is the nominated Privacy Officer for the Institute. The Privacy Officer is responsible for managing compliance with Australian privacy laws, conducting privacy impact assessments and coordinating the Institute's response to data breaches.

33. The Student Services Manager is responsible for the management of student records.

34. All student information handling processes must comply with this Policy and training will be undertaken as part of all staff induction.

Definitions

35. For the purposes of this Policy:

Term	Definition
Personal Information	Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, including a person's name and address, medical records, bank account details, photos, and videos.
Sensitive Information	Personal information about racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, sexual orientation or practices, criminal record, health information.
Records	Any information captured by hard copy, technological or electronic means that pertains to the Institute and its community.
Secure Records	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.
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.
Executive Management Committee	This committee comprises of the CEO, Academic Dean, Registrar, Finance Manager, Marketing Manager, IT Manager

Version history

Version	Changes	Approval Body	Approval Date
1.0	New Policy	Governing Board	
1.1	Point 9, Imperial updated to the Institute Added a row of Staff Personal Information in the table Point 13 c) changed staff to staff / students	Governing Board	19 Sep 2024
1.2	Under Higher education framework added "*National Code of Practice for Providers of Education and Training to Overseas Students 2018* (**National Code**). *Education Services for Overseas Students Act 2000 (ESOS Act)"* Point 26 and 29 replaced "Senior Management Team" with "Executive Management Committee"	GB	27 Feb 2025