1. Purpose

1.1 The primary purpose of a privacy policy at Central Australian Institute of Technology Higher Education (CAIT Hi-Ed) is to ensure the protection and proper management of personal information in compliance with legal and regulatory frameworks. By adhering to the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs), CAIT Hi-Ed aims to uphold the privacy rights of students, staff, and other stakeholders. This includes the collection, use, storage, and disclosure of personal data, ensuring it is handled with transparency, integrity, and accountability.

1.2 Furthermore, the privacy policy supports the CAIT Hi-Ed's commitment to ethical standards and best practices in data management. It provides a framework for addressing privacy-related concerns and complaints, ensuring there are mechanisms in place for individuals to access and correct their personal information.

2. Scope

2.1 This privacy policy applies to a wide range of individuals and entities connected to the institution.

a. Primarily, it encompasses all students, including prospective, current, and former students, ensuring their personal information is handled in accordance with legal and institutional standards.

b. The policy covers university staff, which includes academic, administrative, and support personnel.

c. The privacy policy may also extend to third parties who provides personal information to CAIT Hi-Ed depending on their level of their association. This includes contractors, service providers, and research partners. This policy shall not cover bodies that operate independently of the Institute's governance framework.

3. Policy

3.1 CAIT Hi-Ed is committed to protecting the personal information of its stakeholders through ethical and legal data management practices. All personal and sensitive data will be collected only where necessary, handled lawfully, securely stored, and disposed of in accordance with applicable laws. Individuals will be provided access to their information, with mechanisms to correct inaccuracies, and may lodge complaints concerning data breaches or misuse.

4. Principles

4.1 CAIT Hi-Ed is committed to maintaining openness in its information handling practices. Individuals will be informed about how their personal information is collected, used, stored, and disclosed. Clear, accessible privacy statements and notices will be made available at the point of data collection and on institutional platforms.

4.2 Personal information will only be collected for clearly defined, lawful, and legitimate purposes directly related to CAIT Hi-Ed's educational, administrative, research, or operational functions. Information will not be used or disclosed for any secondary purpose unless the individual has provided consent or where it is permitted by law.

4.3 The collection of personal information will be limited to what is necessary to fulfil the intended purpose. CAIT Hi-Ed will avoid the excessive or irrelevant gathering of information and will periodically review its data collection practices to ensure relevance and necessity.

4.4 Where required, informed consent will be sought before collecting, using, or disclosing personal information. Individuals will be provided with options to give, withhold, or withdraw consent, particularly in contexts such as research participation or promotional communications.

4.5 Individuals have the right to access the personal information that CAIT Hi-Ed holds about them. They may also request corrections if the information is inaccurate, incomplete, or outdated. CAIT Hi-Ed will take reasonable steps to correct such data or annotate the records if correction is not possible.

4.6 CAIT Hi-Ed will implement robust physical, technical, and administrative safeguards to protect personal information against misuse, loss, unauthorised access, modification, or disclosure. Security protocols will be regularly reviewed and updated in line with industry standards and legislative requirements.

4.7 Where appropriate and lawful, individuals will be offered the option to engage with CAIT Hi-Ed anonymously or using a pseudonym. However, in cases where identification is required to provide a service or comply with legal obligations, full identification may be necessary.

4.8 When personal information is transferred outside of Australia, CAIT Hi-Ed will ensure that appropriate contractual, legal, or procedural safeguards are in place. The recipient must be subject to privacy obligations substantially similar to those in Australia, or the transfer must be based on the individual's consent or a lawful exception.

5. Framework and Procedure

5.1 Collecting Information

5.1.1 CAIT Hi-Ed is committed to collecting personal information only when necessary to perform its functions and activities effectively. This includes using data for essential purposes such as:

a. Admission

b. Enrolling in a course

c. Participating in exchange programs,

d. Applying for employment

e. Engage in online forums

f. Registering for events

g. Alumni relations

h. Or general communication through questions or complaints.

5.1.2 CAIT Hi-Ed ensures that any collection of information is conducted through lawful and fair means, avoiding unreasonable intrusion. When information is collected, individuals are informed about the purpose of the collection, how they can access their data, whom it might be disclosed to, whether the collection is legally required, and the potential consequences of not providing the information.

5.1.3 Sensitive information will only be collected under specific circumstances, such as with the individual's informed consent or as mandated by law.

5.1.4 Individual will have to option to remain anonymous while providing the information. However, CAIT Hi-Ed may not be able deliver services as requested.

5.2 Collecting Information Procedure

5.2.1 When collecting information about an individual, CAIT Hi-Ed will follow several key guidelines such as:

a. Collect information only if it is necessary.

b. Gather the information directly from the individual concerned to ensure accuracy and consent.

c. Ensure that the information is collected in a lawful, secure, and fair manner.

d. The process is not unreasonably intrusive, respecting the individual's privacy.

e. Finally, inform individuals that their information is being collected, explain the reasons for the collection, and how the information will be used.

5.2.2 Before or during the time of collecting information, it is crucial to ensure that the individual providing the information is fully informed. Reasonable steps must be taken to make the individual aware of the following key points:

a. Firstly, the individual should know the identity of the organisation collecting the information, whether it is CAIT Hi-Ed or a specific division within CAIT Hi-Ed, and how they can contact the organisation.

b. Secondly, it is important to communicate the purposes for which the information is being collected, such as student enrolment, research, or marketing. Along with this, the individual should be informed about how their information will generally be used and to whom it may be disclosed.

c. Additionally, the individual must be made aware that they have the right to access their information. They should also be informed whether the collection of their information is legally required and understand any consequences of not providing the information, such as CAIT Hi-Ed being unable to provide certain services.

d. Lastly, the individual should be informed that CAIT Hi-Ed has a Privacy Policy available on its website and that there is a Privacy Officer or related who can be contacted for any queries or concerns regarding their information.

5.2.3 When collecting information about an individual from a third party, such as another institution or a parent, CAIT Hi-Ed must first obtain the individual's written permission. This ensures that the individual is aware of and consents to their information being shared.

5.2.4 However, there are certain exceptional circumstances where formal authorisation may not be required. For example, in emergency health situations, it may be necessary to collect information without prior written consent to ensure the individual's well-being.

5.2.5 In all cases where information is collected from someone other than the individual, CAIT Hi-Ed must take reasonable steps to inform the individual about the collection. This includes ensuring they are aware of the key points previously outlined, such as the identity of the organisation collecting the information, the purposes for which it is being collected, how it will be used, their rights to access the information, and any relevant legal requirements.

5.2.6 Sensitive information, as defined in the Privacy and Data Protection Act 2014, includes details about an individual's religious, political, or sexual preferences. This type of information should only be collected if it is essential for CAIT Hi-Ed's operations.

5.2.7 CAIT Hi-Ed may collect sensitive information if it is necessary for research or statistical purposes related to government-funded welfare or educational services, provided there is no practicable alternative.

5.2.8 Additionally, sensitive information shall be collected with the individual's informed consent, if required by law, to prevent or lessen a serious and imminent threat to life or health, or for the establishment, exercise, or defence of a legal claim.

5.3 Use and Disclosure

5.2.1 CAIT Hi-Ed will primarily use or disclose an individual's information for the original purpose for which it was collected. In most instances, this means the information is used solely for the primary reason it was gathered.

5.2.2 However, CAIT Hi-Ed may use and disclose information for a secondary purpose if the secondary use is related to the primary purpose. Additionally, the secondary purpose must be something that the individual would reasonably expect.

5.2.3 In situations beyond these scenarios, CAIT Hi-Ed may use or disclose the information if the individual has given consent or if the disclosure is authorized or required by law.

5.4 Use and Disclosure Procedure

5.4.1 Typically, an individual's information shall be used or disclosed only for the purpose for which it was originally collected.

5.4.2 CAIT Hi-Ed may use or disclose information for a secondary purpose without the individual's consent if the secondary purpose is related to the primary purpose. Additionally, the individual must reasonably expect their information to be used or disclosed for this secondary purpose.

5.4.3 The sensitivity of the information plays a crucial role in shaping the individual's reasonable expectations regarding its use or disclosure.

5.4.4 Information may be used or disclosed for purposes other than the original one provided that the individual has consented, the individual believes that the use or disclosure is necessary to prevent a serious or imminent threat to an individual's life, health, safety, or welfare, or to public health, safety, or welfare, or if such use or disclosure is otherwise authorized or required by law.

5.4.5 If there is no consent from the individual, it is essential to seek advice from a Privacy Officer or officer assigned for such purposes before making any disclosure.

5.4.6 Occasionally, CAIT Hi-Ed may use or disclose non-sensitive information for marketing purposes. When doing so, CAIT Hi-Ed will ensure that individuals can easily opt out of being identified in marketing materials.

5.4.7 When a third party requests information about an individual, the Institute must ensure that the request complies with legal and privacy requirements. The third party must either have the individual's explicit consent or possess a legal entitlement to access the information.

5.4.8 For requests made on behalf of an individual, a signed written authority from the individual is required. This means that personal information cannot be shared with parents, solicitors, or other representatives without proper authorization.

5.4.9 In some cases, the Institute's general privacy statements for staff and students may already cover the necessary permissions for information disclosure. However, when dealing with requests from law enforcement agencies, such as Federal or State Police, it is crucial to forward these requests to a Privacy Officer or a concern official thereon immediately. The Privacy Officer will review the request, determine the appropriateness of disclosure, and ensure that it is properly recorded.

5.4.10 In emergencies where information needs to be shared, such as with medical facilities, it is essential to seek guidance from a Privacy Officer to ensure compliance with privacy regulations.

5.4.11 For routine requests, including those from government agencies, Services Australia, or legal representatives, refer these to the university's Legal Services for proper handling. Subpoenas and court-related requests should also be directed to Legal Services.

5.4.12 Under the Privacy and Data Protection Act 2014 (VIC), a child or young person can exercise their rights independently of a parent or guardian if they have the necessary understanding and intelligence to provide informed consent or make their own decisions. Generally, the CAIT Hi-Ed considers its students mature enough to make their own decisions about the disclosure of their personal information, even if they are under 18 years of age.

5.4.13 As a rule, student personal information should not be disclosed to parents or other family members without the student's explicit consent.

5.4.14 However, there are exceptions to this guideline. For instance, if a student has an intellectual disability or is under a Guardianship Order, different considerations may apply. For any uncertainties or specific cases, please consult Legal Services.

5.5 Cross-Border Disclosure

5.3.1 When staff and agents at CAIT Hi-Ed need to send information outside of Victoria as part of their duties, CAIT Hi-Ed will ensure the following conditions are met:

a. The recipient adheres to principles for fair handling of information that are substantially similar to those upheld by CAIT Hi-Ed.

b. The transfer occurs with the individual's consent, or if obtaining consent is impractical, it should be for the individual's benefit and under circumstances where they would likely consent if possible.

c. The transfer is necessary for fulfilling contractual obligations with the individual or with a third party acting on their behalf.

d. The transfer complies with relevant legislation.

5.3.2 Regarding the assignment and use of identifiers, CAIT Hi-Ed will only assign identifiers to individuals or use those assigned by other organizations in accordance with the Information Privacy Principles (IPPs) or other relevant legislation.

5.6 Cross-Border Disclosure

5.6.1 Once the necessity is established, the destination country and the privacy protections offered by the receiving organisation must be assessed. The recipient must have privacy safeguards substantially similar to the Information Privacy Principles (IPPs) or Australian Privacy Principles (APPs). Where feasible, informed and written consent must be obtained from the individual whose data is to be disclosed. The consent should clearly outline the purpose of the disclosure, the identity of the overseas recipient, the type of personal data involved, and the jurisdiction it will be transferred to.

5.6.2 In circumstances where obtaining consent is impractical—such as where it is clearly for the benefit of the individual—CAIT Hi-Ed may proceed with disclosure only if the individual would reasonably expect it or if it is legally justified. In such cases, the reasons for proceeding without consent must be documented internally.

5.6.3 To safeguard the data, a binding contractual agreement or data transfer arrangement must be put in place with the overseas recipient. This agreement must outline the responsibilities of the recipient regarding the secure handling, use, and storage of the personal data. It should also prohibit any unauthorised onward disclosure and require that any data breaches are promptly reported to CAIT Hi-Ed.

5.6.4 Where personal identifiers are involved (such as student or employee IDs), CAIT Hi-Ed will only assign its own identifiers or use those assigned by other organisations if it is legally authorised to do so. The use of identifiers must align with privacy principles and must not be excessive or unnecessary.

5.6.5 A central register of all cross-border disclosures must be maintained securely. This register should include the date and reason for disclosure, the identity of the individual(s) affected, recipient details, the legal basis or consent for the disclosure, and copies of supporting documentation. Individuals must also be made aware, through the privacy policy or collection notices, that such disclosures may occur in specific situations.

5.6.6 Finally, all overseas data sharing arrangements are subject to annual review to ensure continued legal compliance. Where new technologies or third-party platforms are introduced that may involve cross-border data flows, a Privacy Impact Assessment (PIA) should be conducted to evaluate risks and appropriate controls.

5.7 Access and Correction

5.4.1 CAIT Hi-Ed is committed to providing individuals with access to their personal information, in accordance with legal requirements. Requests for access will be handled in line with applicable legislation such as Freedom of Information Act 1982 (Vic).

5.4.2 In certain situations, individuals may need to make access requests through separate channel. For guidance on any concerns related to information access, individual should reach out to the concern person at CAIT Hi-Ed such as CEO or Academic Dean for assistance.

5.4.3 If an individual identifies that their information is inaccurate, incomplete, or outdated, CAIT Hi-Ed will take reasonable steps to correct the information. Alternatively, CAIT Hi-Ed will record the individual's disagreement with the information if a correction is not feasible.

5.8 Access and Correction Procedure

5.8.1 Individuals wishing to access their personal information held by the Institute must submit a formal request. This request can usually be made in writing, either through a designated online portal or by contacting the Institute's privacy or records management office. The request should include sufficient details to identify the information being sought and verify the identity of the requester.

5.8.2 If an individual believes that their personal information is inaccurate, incomplete, or outdated, they can request a correction. This request should be made in writing and provide details about the necessary corrections. The Institute will review the request and, if justified, amend the information accordingly. If the Institute decides not to make the correction, they must provide the individual with a written explanation and information about how to lodge a complaint.

5.8.3 While CAIT Hi-Ed may charge a fee for accessing information, it should be reasonable and reflect the cost of processing the request. Any fees will be communicated to the requester before processing begins.

5.8.4 Throughout the process, the Institute will ensure that all personal information is handled with confidentiality and in compliance with privacy regulations. Any updates or corrections to personal information will be reflected in the Institute's records and systems promptly.

5.9 Data Security and Disposal

5.5.1 CAIT Hi-Ed staff and associates will be responsible for ensuring that Personal Information under their care is kept secure. This includes protecting the information from unauthorized use, access, disclosure, modification, or loss, whether intentional or accidental.

5.5.2 Additionally, in accordance with the Public Records Act 1973 (Vic) and other relevant legislation, any information that is no longer needed by the Institute shall be either destroyed or permanently de-identified.

5.5.3 Individuals have the right to file a complaint with the Institute if they believe their personal information has been used, accessed, disclosed, or modified without authorisation, whether this occurs deliberately or inadvertently.

5.10 Data Security and Disposal Procedure

5.10.1 CAIT Hi-Ed will implement robust access control measures to ensure that only authorized personnel have access to sensitive or personal information. This includes the use of passwords, encryption, and multi-factor authentication.

5.10.2 Physical access to data storage areas, such as server rooms and filing cabinets, is restricted to authorized staff. Secure facilities and surveillance measures shall be employed to protect physical data assets.

5.10.3 CAIT Hi-Ed will utilise firewalls, antivirus software, and intrusion detection systems to protect against cyber threats. Regular updates and patches will be applied to software and systems to mitigate vulnerabilities.

5.10.4 Sensitive data will be encrypted both at rest and in transit to prevent unauthorized access during storage and transmission.

5.10.5 Information will be classified based on its sensitivity, and appropriate security measures will be applied according to its classification level.

5.10.6 Personal and sensitive data will be stored in secure systems with restricted access. Electronic data will be stored in encrypted databases, while physical documents will be kept in locked, secure locations.

5.10.7 When electronic data is no longer needed, it will be securely deleted using methods that prevent recovery, such as data wiping or degaussing. For storage devices, physical destruction may be used to ensure data cannot be retrieved.

5.10.8 Paper documents containing personal or sensitive information will be shredded or otherwise destroyed to prevent unauthorized access. CAIT Hi-Ed will use secure shredding services for this purpose.

5.10.9 CAIT Hi-Ed will follow retention policies that dictate how long different types of data must be kept before disposal. These policies comply with legal and regulatory requirements and are designed to ensure that data is not kept longer than necessary.

5.10.10 Staff concerned will be trained on data security best practices and the proper handling and disposal of sensitive information. Ongoing training ensures that employees are aware of their responsibilities and any updates to policies.

5.10.11 In the event of a data breach or security incident, CAIT Hi-Ed will have procedures in place for reporting, investigating, and mitigating the impact of the breach. This includes notifying affected individuals and regulatory authorities as required.

5.11 Marketing and Research

5.11.1 CAIT Hi-Ed will only use personal information for direct marketing purposes (such as promoting courses, events, services, or institutional updates) where the individual has provided their explicit consent or where such use is otherwise permitted under the Privacy Act 1988 (Cth)**.**

Individuals will be given clear options to opt in or out of receiving direct marketing communications at the time their information is collected, and in every subsequent communication. CAIT Hi-Ed will honour any request to unsubscribe from such communications promptly and without penalty.

5.11.2 De-identified information—meaning data from which personal identifiers (such as names, student IDs, email addresses, etc.) have been removed—may be used by CAIT Hi-Ed for purposes such as institutional research, program evaluation, quality assurance, strategic planning, and reporting.

5.12 Complaints and Breaches

5.12.1 Complaints Management

Individuals who believe that their personal information has been mishandled—such as being collected, used, disclosed, or stored in breach of applicable privacy laws or institutional policy—have the right to make a formal complaint.

- Complaints should be directed to the CAIT Hi-Ed IT Officer, who is responsible for overseeing compliance with privacy obligations and investigating alleged breaches.
- Complaints must be submitted in writing and should clearly describe the nature of the concern, the information involved, and any supporting details.
- The Privacy Officer will acknowledge receipt of the complaint within a reasonable timeframe and will initiate a confidential investigation.
- The complainant will be informed of the outcome of the investigation and any actions taken to resolve the matter.
- If the complainant is dissatisfied with the outcome, they may escalate the matter to an external body such as the Office of the Australian Information Commissioner (OAIC) or the Victorian Information Commissioner, depending on the jurisdiction.

5.12.2 Data Breach Response Protocol

CAIT Hi-Ed is committed to a timely, transparent, and effective response to actual or suspected data breaches.

In the event of a data breach—defined as any unauthorised access to, disclosure of, or loss of personal information—the following protocol will apply:

5.12.2.1 Containment and Initial Assessment

- The staff member identifying the breach must immediately report it to the Privacy Officer and relevant IT and executive personnel.

- Immediate steps will be taken to contain the breach (e.g., disabling compromised accounts, securing systems, retrieving disclosed documents).

5.12.2.2 Investigation

- A thorough investigation will be conducted to determine the nature, scope, cause, and potential impact of the breach.
- Risk assessments will consider the type of information involved, the number of individuals affected, and the likelihood of harm.

5.12.2.3 Notification

- If the breach is deemed likely to result in serious harm to individuals, CAIT Hi-Ed will notify the affected individuals and report the incident to the OAIC in accordance with the Notifiable Data Breaches (NDB) Scheme under the Privacy Act 1988 (Cth).
- Notifications will include a description of the breach, the types of information involved, recommended steps individuals can take to protect themselves, and contact details for further enquiries.

5.12.2.4 Remediation and Review

- Corrective actions will be implemented to prevent recurrence, such as policy updates, system enhancements, or staff retraining.
- A post-incident review will be conducted to evaluate the effectiveness of the response and update the data breach response plan as needed.

6. Roles and Responsibilities

Chief Executive Officer (CEO)

- Provides strategic oversight and ensures institutional compliance with applicable privacy legislation.
- Supports allocation of resources to maintain and improve privacy protection systems.
- Endorses privacy-related policies, procedures, and corrective actions when breaches occur.

Privacy Officer (or Delegated Officer)

- Acts as the central point of contact for all privacy-related matters.
- Provides advice and guidance to staff and stakeholders on privacy obligations and policy interpretation.
- Oversees implementation and regular review of the privacy policy, procedures, and data handling practices.
- Investigates privacy complaints and suspected breaches of personal information.
- Coordinates breach responses and liaises with external regulators (e.g., OAIC, VIC Information Commissioner) when required.

Information Technology (IT) Officer / Systems Administrator

- Implements and maintains cybersecurity controls to protect electronic personal information.
- Supports breach containment and system-level remediation during privacy incidents.
- Ensures secure storage, access control, encryption, and deletion of electronic records.
- Conducts regular system audits to ensure compliance with data security requirements.

Academic Dean / Heads of Department

- Ensures that data collection, use, and disclosure in academic programs align with privacy legislation and institutional policy.

- Ensures student records and staff information are handled securely and only accessed by authorised personnel.
- Works with the Privacy Officer in responding to access or correction requests related to academic records.

All Staff and Contractors

- Must comply with this policy and the Information Privacy Principles (IPPs) or APPs where applicable.
- Are responsible for protecting the personal information they handle in their roles.
- Must complete privacy training and stay informed of institutional policies and legal requirements.
- Are required to report actual or suspected breaches or mishandling of data to the Privacy Officer immediately.

Students and Stakeholders

- Have the right to be informed about how their personal information is collected, used, and disclosed.
- Must provide accurate and up-to-date information when required by CAIT Hi-Ed.
- Are responsible for exercising their privacy rights, including submitting access or correction requests and lodging complaints where appropriate.

7. Authority and Compliance

File Number	HEP107
Status	Current
Approval Authority	Governance Board.
Legislative Compliance	• Privacy Act 1988 (Cth) • Australian Privacy Principles (APPs) • Information Privacy Principles (IPPs) • Privacy and Data Protection Act 2014 (Vic) • Freedom of Information Act 1982 (Vic) • Public Records Act 1973 (Vic)
Supporting Documents	• CAIT Hi-Ed Personal Information Collection Notice Template • CAIT Hi-Ed Third-Party Information Disclosure Authorisation Form • CAIT Hi-Ed Correction of Personal Information Request Form • CAIT Hi-Ed Privacy Complaint Lodgement Form • CAIT Hi-Ed Privacy Impact Assessment (PIA) Template • CAIT Hi-Ed Cross-Border Data Transfer Risk Assessment Checklist • CAIT Hi-Ed Data Retention and Disposal Register Template • CAIT Hi-Ed Staff Privacy Acknowledgement Form • CAIT Hi-Ed Cross-Border Disclosure Register • CAIT Hi-Ed Marketing Consent/Opt-Out Form
Related Documents	• CAIT Hi-Ed Complaints, Grievance and Appeal Policy and Procedure • CAIT Hi-Ed Information Management Policy and Procedure • CAIT Hi-Ed Staff Code of Conduct • CAIT Hi-Ed Student Code of Conduct

	• CAIT Hi-Ed Marketing and Advertising Policy and Procedure
Higher Education Standards Framework (Threshold Standards) 2021	• Standard 5.3; ss 1 – 1 • Standard 6.2; ss 1 – 2 • Standard 7.1; ss 1 - 3 • Standard 7.2; ss 1 – 4
Education Services for Overseas Students (ESOS Act) and National Code of Practice for Providers of Education and Training to Overseas Students 2018	• Standard 3; ss 1 – 3 • Standard 6; ss 1, 4 & 5 • Standard 7; ss 1 • Standard 8; ss 1 – 3 • Standard 10; ss 1 -2 • Standard 11; ss 1 -2
Responsible Officer	Academic Dean.
Responsible Executive	CEO.
Enquiries Contact	Academic Dean.
Effective Date	
Expiry Date	Not applicable
Next Review	3 Years from the effective date

8. Review Schedule

This policy will be reviewed by the Academic Board every three years.

Version History			
Version No	Approved by	Approval Date	Revision Notes
1.0	Governance Board	16/8/2024	