1. Purpose

1.1 The purpose of this Information Management Policy and Procedure is to provide a structured framework for managing information assets across the Central Australian Institute of Technology Higher Education (CAIT Hi-Ed). As a higher education provider, CAIT Hi-Ed is responsible for collecting, storing, using, and disposing of a wide range of information relating to students, staff, business operations, and marketing activities. This policy aims to ensure that all information is handled securely, ethically, and in compliance with relevant legislative and regulatory requirements.

1.2 This policy also ensures that information is treated as a valuable asset that supports decision-making, continuous improvement, and institutional accountability. It guides the development of robust procedures and practices for the management of information throughout its lifecycle — from creation and collection to disposal or permanent retention — with a strong focus on information integrity, confidentiality, and accessibility.

2. Scope

2.1 This policy applies to all information managed by CAIT Hi-Ed, regardless of its format, location, or method of storage. It covers both physical and electronic records and extends to information managed internally or by external service providers on behalf of the institution. All staff, contractors, and third parties who access or use CAIT Hi-Ed information are required to comply with this policy.

2.2 The policy encompasses academic, administrative, student, and operational information, with procedures tailored to meet the unique requirements and sensitivity of each category. It ensures consistency and standardisation in managing information to uphold legal, regulatory, and institutional obligations.

3. Policy

3.1 CAIT Hi-Ed implements a comprehensive information management system that upholds the principles of transparency, accuracy, privacy, and security. Information is collected and stored in accordance with applicable Australian laws, including the Privacy Act 1988 (Cth), and guidelines provided by the Tertiary Education Quality and Standards Agency (TEQSA).

3.2 The institution adopts a proactive approach to managing information, ensuring that systems and processes are in place to support timely access, accurate classification, and secure sharing of information. Staff are trained and supported in their roles as custodians of information to maintain the highest standards of data quality and stewardship.

3.3 Information governance practices are reviewed regularly to adapt to technological advancements, emerging risks, and evolving educational needs. Continuous improvement and audit processes are implemented to assess the effectiveness of information management strategies and to identify areas for development.

3.4 Any breaches of this policy, including security violations, unauthorised access, or misuse of information, are investigated and may result in disciplinary action, including termination of employment or legal proceedings, depending on the severity of the breach.

4. Principles

4.1 Information is managed as a strategic asset that contributes to CAIT Hi-Ed's vision of delivering quality education and operational excellence. Sound information management practices support informed decision-making, institutional planning, and stakeholder engagement.

4.2 All information collected or generated by CAIT Hi-Ed is treated as confidential unless designated otherwise. The institution implements classification and access controls to protect sensitive information and mitigate the risk of data breaches, identity theft, and reputational damage.

4.3 The lifecycle of information is documented and governed by clearly defined stages: planning and strategy, collection, classification, storage, usage, maintenance, retention, and final disposal. Each stage has embedded quality control mechanisms to ensure data integrity and compliance.

4.4 Technology and infrastructure used to manage information are secure, fit-for-purpose, and regularly updated to address emerging cybersecurity threats. Staff are provided with tools and resources to manage information efficiently within their respective departments.

4.5 The policy also prioritises transparency and accountability in information sharing with students, regulators, and other stakeholders. Information shared externally is subject to rigorous checks to prevent unauthorised disclosure.

4.6 Roles and responsibilities for managing information are clearly defined and communicated across the organisation. All individuals handling information are expected to uphold the institution's standards and undergo periodic training.

5. Information Categories

CAIT Hi-Ed will categorise information into five primary domains (it can increase as the Institute grows) to ensure appropriate handling based on sensitivity, purpose, and regulatory obligations. Each category will be managed in alignment with the institution's risk management, privacy, and security protocols.

5.1 **Business Information**

It will include strategic plans, governance records, contracts, financial reports, procurement documents, and internal communications. This type of information will be highly sensitive due to its potential impact on institutional operations and reputation. Risks may include operational disruption, financial loss, and reputational damage. It will be controlled through strict access protocols, audit trails, and systems that allow for traceable and reviewable changes.

5.2 Marketing Information

It will comprise advertising strategies, campaign metrics, branding guidelines, social media content, public relations materials, and market research. Additionally, it will include a publicly accessible repository of current and accurate information about CAIT Hi-Ed's operations, courses, and compliance status. This repository will detail the provider's registered and trading names, regulatory authority, governance structure, financial standing, enrolment figures, and organisational framework. It will also include comprehensive listings of campuses and facilities, course offerings and enrolments, partnerships for course delivery, recent public annual reports, complaints procedures, and contact information.

Each course listed in the repository will include accreditation details, qualification levels, AQF recognition, professional accreditation (where applicable), authorisation for delivery to international students, course duration, and applicable credit transfer or RPL policies. This type of marketing information, while moderate in sensitivity, will be critical for transparency, regulatory compliance, and maintaining trust with prospective students and stakeholders. To safeguard this information, CAIT Hi-Ed will employ content management systems, version control, and access controls to ensure accuracy and proper governance.

5.3 Student Information

It will encompass personally identifiable data such as names, addresses, birthdates, student IDs, enrolment records, academic results, financial aid details, and incident reports. This information will be classified as highly sensitive, given its implications under privacy legislation and the potential for identity theft or privacy breaches. Protective measures will include encryption, secure communication channels, consent-based sharing, and strict access based on role and necessity.

5.4 Staff Information

It will consist of employment contracts, resumes, leave records, tax file numbers, payroll records, performance reviews, and health-related documentation. Like student data, this category will be considered highly sensitive. Risks such as legal non-compliance, industrial disputes, or staff dissatisfaction will be mitigated through access limitation to authorised HR personnel and supervisors, along with ongoing compliance audits and secure data handling practices.

5.5 Third-Party Information

It will relate to data shared by or received from external partners, contractors, regulatory bodies, service providers, and research collaborators. The sensitivity of this data will vary depending on its nature and associated contractual obligations, but it may include proprietary or confidential material. Key risks will include breaches of contract, legal liabilities, and damage to institutional relationships. Controls will include binding data-sharing agreements, non-disclosure agreements (NDAs), secure data access mechanisms, and adherence to relevant privacy and cybersecurity standards.

6. Storage and Security

Information will be stored using both physical and digital methods, and CAIT Hi-Ed will implement appropriate security measures tailored to each medium to ensure confidentiality, integrity, and availability of information assets.

6.1 Physical Storage:

Physical records, such as printed documents, contracts, personnel files, and archived materials, will be stored in secure, access-controlled environments. Storage facilities will include lockable filing cabinets, restricted-access rooms, and onsite archives. Only authorised staff members will be permitted to access physical records, and access logs or sign-out registers will be maintained to monitor movement of documents. Fire protection, environmental controls, and disaster recovery measures will be incorporated to mitigate risks such as theft, damage, or loss due to natural disasters.

6.2 Digital Storage:

Digital information will be stored on secure servers, cloud-based platforms, and institutional databases. All digital storage systems will be protected through multilayered security protocols including password protection, role-based access control, data encryption, and firewalls. Critical systems will use multifactor authentication and maintain regular backups to ensure continuity and recovery. Access to digital information will be logged, monitored, and periodically reviewed to detect unauthorised access or anomalies.

6.3 Security Breaches:

In the event of a security breach, whether physical or digital, CAIT Hi-Ed will activate its incident response plan. This will involve identifying and containing the breach, notifying relevant authorities and stakeholders, conducting a full investigation, and implementing corrective measures. Staff will receive regular training on information security awareness, and periodic audits will be conducted to test the resilience of both physical and digital security systems.

7. Procedure

7.1 Planning and Strategy

7.1.1 Information planning will be integrated into institutional strategy development and project initiation phases.

7.1.2 Each business unit will identify its information needs, outline the types of data it will handle, and establish appropriate governance structures.

7.1.3 Information management plans will define objectives, identify regulatory and compliance requirements, establish roles and responsibilities, and address associated risks and mitigations.

7.1.4 Planning will also include forecasting for data volume growth and future storage or security needs.

7.2 Information Creation and Collection

7.2.1 Information will be created or collected ethically, lawfully, and in alignment with business or academic needs.

7.2.2 Data collection methods will include digital forms, enrolment platforms, surveys, applications, and internal communications.

7.2.3 All collected information will be validated for accuracy at the point of entry.

7.2.4 Mechanisms will be in place for updating and correcting information on an ongoing basis.

7.2.5 Staff will be responsible for ensuring information remains accurate and complete throughout its lifecycle.

7.3 Organisation and Classification

7.3.1 All information will be organised and classified according to its sensitivity, format, source, and intended use.

7.3.2 A standard classification scheme (e.g., Public, Internal, Confidential, Restricted) will be adopted and applied consistently.

7.3.3 Metadata tagging, file naming conventions, and indexing protocols will support easy retrieval, archiving, and access management.

7.3.4 The classification system will be documented and regularly reviewed to ensure it remains aligned with legal and operational requirements.

7.4 Storage and Access Control

7.4.1 Information will be stored either physically or digitally, with controls proportionate to the classification level.

7.4.2 Physical storage will involve secure facilities with locked cabinets and restricted access.

7.4.3 Digital storage will involve secure servers, cloud platforms, and encrypted databases.

7.4.4 Role-based access controls will restrict access to only those with a business or academic need.

7.4.5 All access will be logged, and unusual or unauthorised access attempts will be investigated promptly.

7.4.6 Staff will undergo regular training in secure access protocols.

7.5 Use and Sharing

7.5.1 Information will only be used for its intended and approved purpose.

7.5.2 Internal sharing will follow approval workflows and respect classification levels.

7.5.3 External sharing will require authorisation, and in many cases, formal agreements such as data-sharing arrangements or non-disclosure agreements (NDAs).

7.5.4 Where information involves personal data, consent will be sought and documented.

7.5.5 Usage audits will be conducted to ensure adherence to policy, and breaches will be addressed according to disciplinary procedures.

7.6 Maintenance and Quality Control

7.6.1 Information assets will be reviewed periodically to ensure they remain relevant, accurate, and complete.

7.6.2 Obsolete, duplicate, or inaccurate data will be flagged for correction or deletion.

7.6.3 Each department will maintain a quality control register and ensure information undergoes verification checks, particularly where it informs reporting, compliance, or external publication.

7.6.4 Quality assurance activities will be coordinated by the Information Governance Officer.

7.7 Retention and Disposal

7.7.1 Information will be retained in accordance with legal, regulatory, and institutional retention timelines:

- Student academic records: permanently retained.
- Financial records: retained for a minimum of 7 years.
- Employment and HR records: retained for at least 7 years after termination.
- Incident and complaint records: retained for 7 years following resolution.
- General administrative documents: retained for 5 years unless otherwise required.

7.7.2 Records that are no longer required will be securely destroyed or archived in accordance with classification and regulatory guidelines.

7.7.3 During business cessation, a formal data wind-down plan will be activated, involving stakeholder consultation, record preservation (for compliance and auditing), and secure destruction of remaining information.

7.7.4 Disposal will be documented and, where necessary, conducted by licensed third-party providers.

7.8 Compliance and Security

7.8.1 All staff will be required to comply with this policy.

7.8.2 Non-compliance will result in disciplinary action, up to and including termination of employment.

7.8.3 Security controls will include encryption, antivirus software, firewall configurations, penetration testing, and secure configuration management.

7.8.4 Data breaches will be managed under a formal incident response plan, with reporting obligations to relevant authorities where applicable under the Privacy Act 1988 (Cth).

7.9 Monitoring and Review

7.9.1 Information practices will be continuously monitored through scheduled audits, user access reviews, incident trend analysis, and stakeholder feedback.

7.9.2 The Information Governance Officer will coordinate annual reviews of the policy and its procedures to ensure alignment with emerging risks, technologies, and compliance obligations.

7.9.3 Recommendations from internal and external audits will be used to drive improvements.

8. Roles and Responsibilities

8.1 Information/Compliance Officer

- Oversees the implementation and review of the Information Management Policy.
- Ensures alignment with institutional strategic goals and compliance with regulatory requirements.
- Coordinates training programs and awareness initiatives related to information governance.
- Leads investigations into security breaches and policy violations.

8.2 Department Heads and Managers

- Ensure that staff within their departments adhere to the information management procedures.
- Identify specific information needs and manage records according to classification and retention schedules.
- Report any issues or breaches in information management practices to the Information/Compliance Officer.

8.3 IT Department

- Maintains and secures the digital infrastructure used for storing and managing information.
- Implements and monitors cybersecurity measures including firewalls, encryption, access control, and backups.
- Provides technical support and system access management aligned with user roles.
- Assists in conducting internal audits and risk assessments.

8.4 All Staff Members

- Handle information in accordance with the classification, access, and privacy requirements.
- Participate in information management training and apply best practices in their daily tasks.
- Promptly report data quality issues, security concerns, or policy breaches.
- Ensure records are accurately maintained and updated as needed.

8.5 Contractors and Third-Party Providers

- Adhere to CAIT Hi-Ed's information handling standards and contractual data security obligations.
- Limit access to information strictly to what is necessary for fulfilling their contractual roles.
- Participate in induction or training on the institution's information governance framework when required.
- Cooperate in audits and reviews involving shared or outsourced information systems.

8.6 Students (where applicable)

- Provide accurate personal and academic information during enrolment and throughout their studies.
- Comply with information usage guidelines set out in student policies.
- Report discrepancies or concerns related to their personal data.
- Respect confidentiality and data protection obligations when accessing institutional information systems.

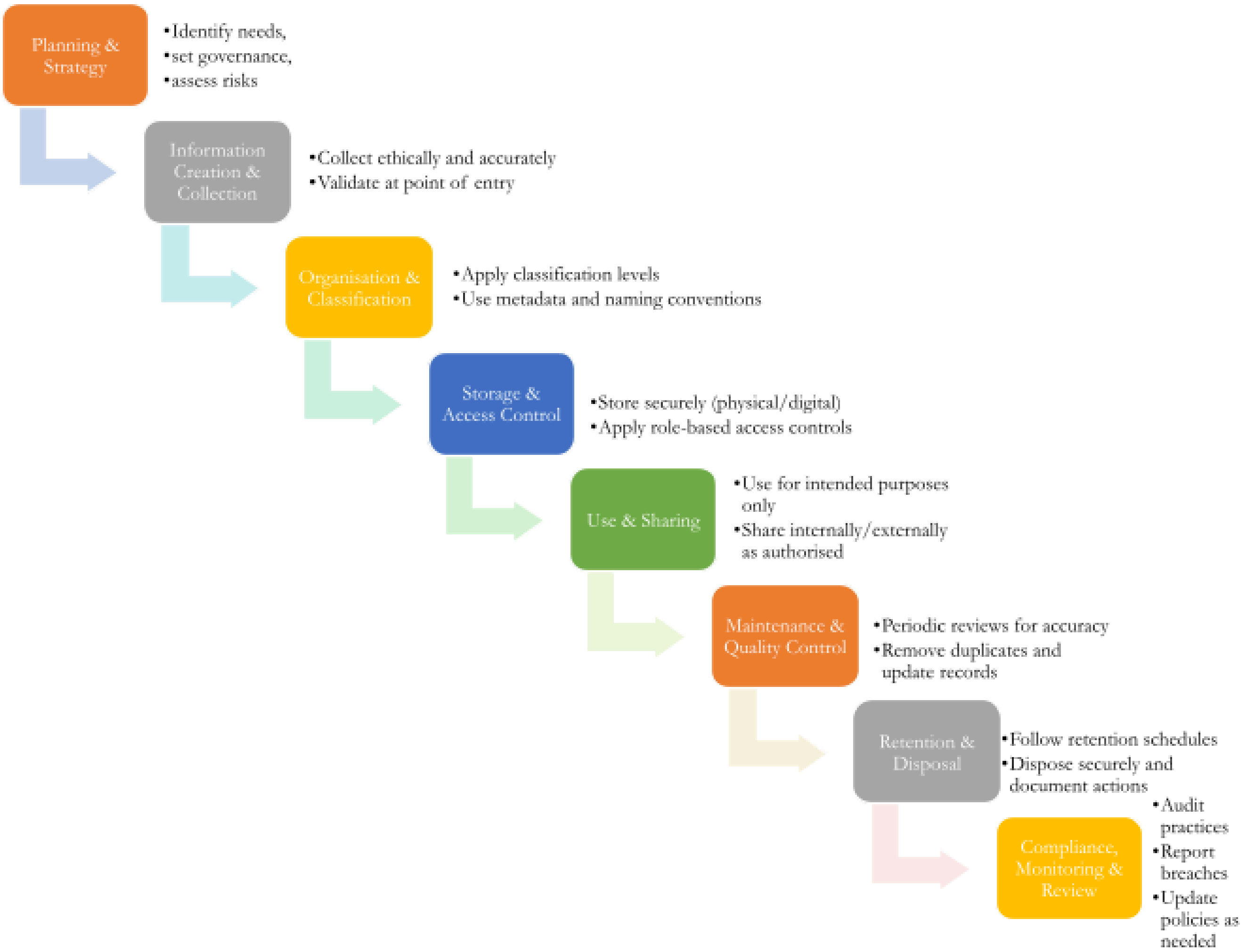
9. Authority and Compliance

File Number	HEP65
Status	Current
Approval Authority	Governance Board.
Legislative Compliance	● Privacy Act 1988 (Cth) ● Tertiary Education Quality and Standards Agency Act 2011 (TEQSA Act) ● Higher Education Standards Framework (Threshold Standards) 2021

	● Archives Act 1983 (Cth) ● Freedom of Information Act 1982 (Cth) ● Copyright Act 1968 (Cth) ● Spam Act 2003 (Cth) ● Electronic Transactions Act 1999 (Cth) ● Fair Work Act 2009 (Cth) ● Notifiable Data Breaches (NDB) Scheme ● AS ISO/IEC 27001:2023 (Information Security Management Standards)
Supporting Documents	• CAIT Hi-Ed Information Access Request Form • CAIT Hi-Ed Information Classification Form • CAIT Hi-Ed Data Breach Notification Form • CAIT Hi-Ed Third-Party Access Request Form • CAIT Hi-Ed Consent to Disclose Personal Information Form • CAIT Hi-Ed IT Access Change Request Form • CAIT Hi-Ed Records Retention Schedule Template • CAIT Hi-Ed Data Sharing Agreement Template • CAIT Hi-Ed Confidentiality Agreement Template • CAIT Hi-Ed Information Asset Register Template • CAIT Hi-Ed Audit Checklist Template (Information Management) • CAIT Hi-Ed Information Management Strategy Document • CAIT Hi-Ed Staff and Student On boarding Information Security Guide • CAIT Hi-Ed Digital Backup and Archiving Procedure
Related Documents	• CAIT Hi-Ed Risk Management Framework / Policy and Procedure • CAIT Hi-Ed Student Grievance and Complaints Policy and Procedure • CAIT Hi-Ed Privacy Policy and Procedure • CAIT Hi-Ed Business Continuity Plan • CAIT Hi-Ed Compliance Management Policy and Procedure. • CAIT Hi-Ed Critical Incident Policy and Procedure
Higher Education Standards Framework (Threshold Standards) 2021	• Standard 2.1; ss 1 - 2 • Standard 3.3; ss 1 - 2 • Standard 3.5; ss 2 • Standard 4.2; ss 1 • Standard 5.2; ss 1 • Standard 6.2; ss 1 • Standard 6.3; ss 1 • Standard 7.1; ss 3 • Standard 7.2; ss 2 • Standard 7.3; ss 1 - 3
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 3 & 5 • Standard 6; ss 9 • Standard 7; ss 4 • Standard 8; ss 3 • Standard 9; ss 3 • Standard 10; ss 6 • Standard 11; ss 1 - 3
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

10. Appendix 1: Information Management Procedure Flow Chart



Planning & Strategy

- Identify needs,
- set governance,
- assess risks

Information Creation & Collection

- Collect ethically and accurately
- Validate at point of entry

Organisation & Classification

- Apply classification levels
- Use metadata and naming conventions

Storage & Access Control

- Store securely (physical/digital)
- Apply role-based access controls

Use & Sharing

- Use for intended purposes only
- Share internally/externally as authorised

Maintenance & Quality Control

- Periodic reviews for accuracy
- Remove duplicates and update records

Retention & Disposal

- Follow retention schedules
- Dispose securely and document actions

Compliance, Monitoring & Review

- Audit practices
- Report breaches
- Update policies as needed

11. Review Schedule

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

Version History			
Version No	Approved by	Approval Date	Revision Notes
1.0	Governance Board	9/5/2025	