Information and Records Management Policy and Procedures

Purpose

The purpose of this Policy is to establish a consistent, compliant, and systematic framework for the creation, management, protection, access, retention, and disposal of information and records held by the Central Institute of Technology and Innovation (the Institute). This Policy ensures that student records, including those of overseas students, are managed in accordance with the ESOS Act 2000, the National Code 2018, privacy legislation, and relevant state and Commonwealth record-keeping obligations.

Scope

This Policy applies to all Institute data, information, and records, whether received, created, maintained, accessed, copied, disseminated, stored, archived, or disposed of by the Institute in the course of its operations. This includes, but is not limited to:

- Student records (domestic and overseas students)
- Academic, administrative, and financial records
- Records created or held by educational agents on behalf of the Institute
- Records managed by third-party service providers under contractual arrangements

Related Documents

This policy should be read in conjunction with the following Institute documents:

- Information Systems Management and Security Policy and Procedures
- Risk Management Policy and Procedures
- Third Party Policy and Procedures
- Acceptable Use of IT Policy and Procedures
- Conflict of Interest Policy and Procedures
- Code of Conduct Policy and Procedures
- Student Code of Conduct Policy and Procedures
- Information and Privacy Policy and Procedures

All documents referenced in this policy can be accessed via the CITI website.

Definition of Key Terms

For the purpose of this Policy, the following definitions apply:

Term	Definition
Staff Member	Any person who is an employee of the Institute. This includes full-time, part-time, sessional and casual staff.
Information Owner	An Information Owner is the person who is responsible and accountable for information and records management for an organisational unit of the Institute and who will ensure appropriate storage, access, use, distribution and disposal of the information and records.
Personal information	Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances. Some examples are: • an individual's name, signature, address, phone number or date of birth. • sensitive information (see below)

Term	Definition
	• financial or credit information • government identifiers e.g., passport number • photographs, video or voice recordings • internet protocol (IP) addresses • voice print and facial recognition biometrics • location information from a mobile device.
Sensitive Information	Sensitive information is personal information relating to an individual's: • health • racial or ethnic origin, including country of birth • political opinions • membership of a political association • religious beliefs or affiliations • philosophical beliefs • membership of a professional or trade association • membership of a trade union • sexual orientation or practices • criminal record • child related employment screening reports
Personal data	Personal data means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural, or social identity of that natural person.

Term	Definition
Reasonably Practicable	Reasonably practicable means that which is, or was at a particular time, reasonably able to be done to ensure that a data breach does not occur, taking into account and weighing up all relevant matters.
Third Party	A Third Party is an organisation, person, or other body, other than the Institute who is normally engaged by the Institute for the provision of a specified service.
Record	A "record" is defined in section 3 of the Privacy and Personal Information Protection Act 1988as: "any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means".
Strictly Confidential	Strictly confidential means used for highly sensitive information. Access is strictly limited to a selected group or process access. The distribution, retention, and/or destruction of information is subject to restrictive regulatory obligations and if compromised, would place the Institute in breach of its legal and regulatory responsibilities.
Restricted to Staff	Restricted to staff means information available to staff who need access to fulfill their operational duties but is not for public disclosure.
Restricted to Staff and Students	Restricted to staff and students means information available to staff and students to enable operations, but not for public disclosure.
Public	Public means available to the general public. No adverse effects are expected to result from the wide circulation of this information.
Privacy breach	Occurs when there is a failure to comply

Term	Definition
	with this Policy. Usually, this will result in unauthorised disclosure of or unauthorised access to personal information.
Student Record	Student Record means any information or document relating to a student that is created or received by the Institute, including enrolment details, academic progress, assessments, attendance, welfare and support interventions, communications, complaints, appeals, and visa-related records.
Overseas Student Record	Overseas Student Record means a student record relating to an overseas student, including Confirmation of Enrolment (CoE), PRISMS reporting, course progress, attendance monitoring, deferment, suspension, cancellation, and compliance-related correspondence.
Educational Agent	Educational Agent means an individual or organisation contracted by the Institute to recruit students on its behalf, whether onshore or offshore.

Policy Principles

The Institute manages information and records in accordance with the State Records Act 1998 (NSW), the Privacy Act 1988 (Cth), the ESOS Act 2000, and the National Code 2018.

The Institute will not:

1. Dispose of records prior to the approved retention period.
2. Transfer ownership of records without proper authorisation.
3. Remove records from Institute custody without approval.

4. Alter, damage, or falsify records.
5. Neglect records in a manner that compromises integrity or accessibility.

The Institute will ensure that:

1. All records created or received in the course of Institute business are Institute assets.
2. Records are stored securely and managed in accordance with approved classification levels.
3. Personal and sensitive information is protected from unauthorised access, disclosure, loss, or misuse.
4. Records management practices meet legislative and regulatory requirements.
5. Each record has a clearly identified Information Owner accountable for its management.

Policy Statement

1. Management of Records

In order to ensure the safe management of records, the following apply:

1.1 No Institute information will be sold or have ownership transferred to a third party without the approval of the Chief Executive Officer, or delegate.

1.2 The Institute will manage its records throughout their lifecycle to ensure that they are a complete and accurate record of its business activities and that they remain the property of the Institute.

1.3 Operations maintains an information and records management program that includes:

1.3.1 Information Management.

1.3.2 Principles and guidelines, including requirements for information classification.

1.3.3 Education and training activities for staff.

1.3.4 A retention schedule, including instructions about the disposal and archiving requirements for records.

1.4 To ensure that the confidentiality, integrity, and availability of information is protected, staff will only be provided with access to data and information in accordance with the requirements of their particular role.

2. Student Records (Domestic and Overseas Students)

2.1 The Institute will maintain accurate, complete, and up-to-date student records, including academic progress, attendance, welfare interventions, and outcomes.

2.2 Overseas student records will be maintained in accordance with the ESOS Act and National Code, including:

2.2.1 Confirmation of Enrolment (CoE) details.

2.2.2 PRISMS reporting records.

2.2.3 Course progress and attendance monitoring.

2.2.4 Records of deferment, suspension, cancellation, and appeals

2.2.5 Records of support services and wellbeing considerations.

2.3 Student records will be retained for the period required under legislative and regulatory obligations and will be made available to regulatory authorities upon request.

3. Educational Agents and Third Parties

Educational agents must comply with this Policy and any applicable privacy, ESOS, and National Code requirements.

Contracts with educational agents must include obligations relating to:

3.1.1 Secure handling of student information.

3.1.2 Accurate record creation and transfer to the Institute.

3.1.3 Confidentiality and data protection.

3.1.4 Timely provision of records for audit or regulatory review.

3.2 The Institute retains ultimate responsibility for the accuracy, integrity, and availability of student records created or managed by agents.

4. Privacy, Security, and Breaches

4.1 **Handling of Personal and Sensitive Student Information:** All personal, academic, and sensitive information collected, stored, or processed by the Institute in relation to students including international students will be managed in strict accordance with the Information and Privacy Policy and Procedures, the ESOS Act 2000, the National Code 2018, and other relevant privacy legislation. Information will only be collected for legitimate education-related purposes, maintained accurately, and used solely for authorised functions, including enrolment, course progression, reporting to regulatory bodies (e.g., PRISMS), and provision of support services. Special consideration will be given to sensitive student information, including health records, visa documentation, financial information, and records relating to complaints, appeals, or critical incidents.

4.2 **Breach Reporting and Management:** Any actual, suspected, or potential privacy breach affecting student records whether through loss, unauthorised access, disclosure, or alteration must be reported immediately to Operations or their delegate. The Institute will respond in accordance with the Privacy

Breach Response Procedure (Appendix 1), including:

4.2.1 Investigating the cause and scope of the breach.

4.2.2 Containing and mitigating the impact on affected students.

4.2.3 Notifying affected students and relevant regulatory authorities as required under ESOS, National Code, or privacy legislation.

4.2.4 Implementing measures to prevent recurrence.

4.2.5 All breaches will be formally recorded, reviewed, and used to inform improvements to the Institute's student records management and risk mitigation strategies.

4.3 **Confidentiality of Student Records:** Records relating to student wellbeing, academic progression, complaints, appeals, disciplinary matters, or critical incidents will be treated as strictly confidential.

4.3.1 Access is limited to authorised personnel on a need-to-know basis.

4.3.2 Confidential records will be securely stored with role-based access controls, encryption where required, and adherence to retention schedules aligned with ESOS obligations.

4.3.3 Staff, contractors, and third parties are required to comply with these standards as a condition of engagement with the Institute.

4.4 **Security of International Student Data:** International student data, including personal, visa, and CoE information, will be subject to heightened security measures to comply with ESOS and National Code requirements.

4.4.1 Systems and processes will ensure that student data is accurate, up-to-date, and reported correctly to regulatory bodies (such as PRISMS), and that any changes to enrolment, course duration, or leave of absence are recorded promptly.

4.4.2 The Institute will regularly audit these systems to verify compliance and data integrity.

4.5 **Technical, Administrative, and Physical Safeguards:** The Institute will implement appropriate safeguards to protect student records against unauthorised access, alteration, disclosure, or loss.

4.5.1 Measures include secure digital storage, password-protected systems, network security protocols, controlled physical access to records, and ongoing staff training on data privacy, ESOS compliance, and National Code obligations.

4.6 **Continuous Improvement and Compliance Monitoring:** The Institute will monitor compliance with privacy, security, and student records requirements through regular audits, risk assessments, and policy reviews.

4.6.1 Lessons learned from breaches, near misses, or regulatory feedback will be used to strengthen records management practices, ensuring ongoing compliance with ESOS and the National Code while protecting the rights and welfare of all students.

5. Website Data and Information

5.1 **Accuracy and Currency of Information:** The Institute's website serves as a primary source of information for prospective and enrolled students, including international students.

5.1.1 All data and content published on the website, including course descriptions, admission requirements, fees, policies, procedures, and student support information, must be accurate, complete, and up-to-date.

5.1.2 The website will reflect any changes to course offerings, CRICOS registration, policies, or procedures in a timely manner to ensure compliance with the ESOS Act 2000 and the National Code 2018.

5.2 **Privacy and Collection of Data:** Any personal information collected via the website, such as enquiries, applications, or contact forms, will be handled in accordance with the Institute's Information and Privacy Policy and Procedures.

5.2.1 The collection, storage, and processing of personal data must comply with ESOS and National Code requirements, including appropriate consent, secure handling, and restrictions on use and disclosure.

5.3 **Accuracy of Student Recruitment Information:** Information provided to prospective international students must not be false or misleading.

5.3.1 This includes course details, admission requirements, fees, pathways, and student support services.

5.3.2 Website content will be regularly reviewed and approved by relevant Information Owners and Operations to ensure accuracy, clarity, and regulatory compliance.

5.4 **Accessibility and Transparency:** The website must provide clear access to key documents, including the Student Handbook, Course Rules and Progression Policy, fees information, and policies related to deferral, suspension, cancellation, and complaints.

5.4.1 Links and references to external resources, such as government cost-of-living calculators or visa information, should be functional, accurate, and current.

5.5 **Security of Website Data:** Technical and administrative safeguards must be implemented to protect website data from unauthorised access, modification, or loss.

5.5.1 Security measures include encrypted communications, secure login systems for restricted areas, regular system backups, and monitoring for potential breaches or vulnerabilities.

5.6 **Continuous Review and Compliance:** Website data and content will be audited regularly to ensure continued compliance with ESOS, the National Code, and the Institute’s internal policies.

5.6.1 Any errors, outdated content, or non-compliant information identified will be corrected promptly, and lessons learned will be applied to strengthen ongoing website governance practices.

Procedures

The following procedures apply to this Policy and form part of the Institute's governance framework for information and records management. These procedures ensure that information is managed responsibly, stored securely, retained appropriately, and disposed of lawfully. Supporting these procedures, the Privacy Breach Response Procedure (Appendix 1) provides a clear process for responding to a Privacy Breach.

1. Information Management Framework

1.1 Operations and other relevant organisational units, will develop, maintain, and promote the Institute's Information Management Framework. This framework includes policies, procedures, classification guidelines, and record-keeping protocols that support the responsible management of all forms of data and records — digital, physical, personal, sensitive, and institutional.

1.2 Operations is also responsible for facilitating regular training and awareness programs for all staff, contractors, and third-party providers. These programs will cover legal obligations under the Privacy Act 1988, State Records Act 1998 (NSW), the Higher Education Standards Framework (2021), and internal policies and procedures. Training will occur at induction, during role changes, and at scheduled intervals thereafter (at least annually).

1.3 Information Owners (typically senior leaders within departments) will ensure that proper practices for creating, capturing, storing, sharing, and disposing of records are in place for their organisational unit. They are accountable for applying correct information classification, ensuring access permissions are updated promptly, and that compliance requirements are upheld in their areas of responsibility.

1.4 Supervisors and Managers must verify that all staff, contractors, and volunteers under their direction are:

1.4.1 Trained in records management expectations relevant to their position.

1.4.2 Aware of the information classification levels and appropriate labelling.

1.4.3 Equipped to follow appropriate access and storage protocols.

1.4.4 Supported in raising concerns or reporting non-compliance.

1.4.5 Where issues or gaps are identified, the relevant supervisor must notify Operations and participate in resolving the issue in line with the Institute's Continuous Improvement and Risk Management frameworks.

2. Information Classification

2.1 All staff, including contractors and volunteers, must classify and manage information in accordance with the Institute's classification schema. This classification is essential to preserve the confidentiality, integrity, and availability of Institute records, and to prevent the unauthorised access, use, alteration, or destruction of information.

2.2 Records must be classified at the time they are created, received, or processed. Staff must apply the classification that best corresponds to the content and sensitivity of the information. Where there is uncertainty, the record must be handled using the most restrictive classification level until the Information Owner provides definitive classification guidance.

2.3 All information and records must be clearly labelled using one of the following Institute-approved classifications:

2.3.1 **Strictly Confidential:** Information of the highest sensitivity. Access is restricted to authorised personnel only. Breach of confidentiality could lead to legal, reputational, or operational harm (e.g. student misconduct files, board deliberations, legal contracts).

2.3.2 **Restricted to Staff: I**nternal information used by staff to fulfil business functions but not suitable for broader dissemination (e.g. operational reports, internal audits, HR policies).

2.3.3 **Restricted to Staff and Students:** Information accessible to both staff and students where appropriate for learning, engagement, or operations (e.g. subject outlines, timetables).

2.3.4 **Public:** Information that is authorised for release into the public domain (e.g. website content, published course brochures).

2.4 The Institute's recordkeeping systems will include metadata elements that capture the classification level, record ownership, creation/modification dates, and access control status for each entry. Classification should be reviewed periodically, particularly when information is repurposed, shared externally, or transferred to archive.

2.5 Misclassification of records, whether deliberate or inadvertent, will be treated as a breach of this Policy and may lead to disciplinary or corrective action, especially if it results in unauthorised disclosure or legal/regulatory consequences.

3. Information Storage

3.1 All confidential, personal, sensitive, and proprietary information must be stored securely using systems and platforms that comply with the Institute's Acceptable Use of IT Policy and Procedures, and in accordance with relevant legislation and best practice information governance standards. Information must be protected against unauthorised access, corruption, loss, or destruction throughout its entire lifecycle.

3.2 **Primary storage** of all institutional records must be located within approved, secure systems maintained by the Institute's IT Services or contracted providers under formal agreements with defined data security obligations. These systems must include automated backup, audit logs, access control mechanisms, and redundancy provisions to ensure business continuity and disaster recovery.

3.2.1 **Electronic records** must be stored in secure digital repositories that provide:

3.2.2 Password protection and multi-factor authentication.

3.2.3 Role-based access controls, where users are granted the minimum level of access necessary to perform their duties.

3.2.4 Encryption of data in transit and at rest.

3.2.5 Regular system and software updates to protect against vulnerabilities.

3.2.6 Activity logging and monitoring to track access, modifications, and deletions.

3.3 **Hard copy records** containing sensitive or confidential information must be stored in locked cabinets or rooms with restricted access. These records must be registered in the Institute's records management system and subject to the same classification and retention rules as digital records.

3.4 Where staff are required to temporarily store confidential information on portable storage devices (e.g. USBs, laptops, external hard drives), those devices must:

3.4.1 Be provided or approved by the Institute.

3.4.2 Have appropriate encryption and password protection.

3.4.3 Be physically secured when not in use.

3.4.4 Be scanned for malware regularly and returned to a secure institutional system as soon as practicable.

3.5 **Cloud storage solutions** or third-party platforms may only be used when approved by the Chief Executive Officer (or delegate) and subject to a documented data protection agreement. These services must:

3.5.1 Be hosted in data centres that comply with Australian data sovereignty requirements (where applicable).

3.5.2 Offer enterprise-grade security features.

3.5.3 Be formally assessed for risk prior to use.

3.6 **Email, collaboration tools, and mobile devices** must not be used to store or transmit personal or sensitive data unless they are specifically configured for secure handling and meet institutional standards. Where inappropriate use is identified, Operations will work with the responsible staff member to mitigate the risk and ensure corrective action is taken.

3.7 **Staff Responsibilities:** Staff are responsible for ensuring that working documents and personal files are stored in authorised locations and not left on personal desktops, unprotected folders, or personal devices that fall outside the control of the Institute's systems.

3.8 **Information Owners:** Information Owners must conduct periodic audits of stored data (at least annually) to ensure information is current, classified appropriately, and retained or archived in accordance with the retention schedule.

4. Access

Access to information and records held by the Institute will be based strictly on the principle of "least privilege," meaning that individuals are granted access only to the information necessary to perform their duties.

4.1 Permission levels are determined by the individual's role and responsibilities and are configured to prevent unauthorised access to confidential, personal, academic, or sensitive information.

4.2 Role-based access rights are reviewed and revalidated at least annually by Operations (or delegate), and more frequently if there are changes in staff responsibilities, employment status, or organisational structure.

4.3 Requests for additional access must be justified by a legitimate business need, submitted through a formal process to Operations, and approved by the Chief Executive Officer or an authorised delegate.

4.4 All access activity is monitored and logged, with audit trails maintained for a minimum of seven years to detect and investigate unauthorised or inappropriate use.

4.5 Multi-factor authentication and password security protocols are enforced to provide an additional layer of protection to critical systems, including the Student Management System, Learning Management System, Human Resources System, and other enterprise databases.

5. Disposal

The disposal of records must be consistent with the Institute's Retention and Disposal Schedule, developed in alignment with the State Records Act 1998 (NSW), TEQSA guidance, and applicable Commonwealth legislation.

5.1 No staff member is permitted to dispose of, delete, or destroy any physical or electronic record without the prior written approval of Operations.

5.2 All disposal must be documented, and the method of disposal (e.g., shredding, secure deletion) must ensure that no part of the record is retrievable.

5.3 Records must never be destroyed if:

5.3.1 They are subject to legal proceedings or reasonably anticipated litigation.

5.3.2 They relate to a formal complaint, incident, or appeal still under review.

5.3.3 A statutory or regulatory request for access has been made (e.g., under the Privacy Act 1988 or Freedom of Information Act 1982).

5.3.4 Their disposal would breach an agreement or condition placed on the Institute (e.g., by TEQSA, ASQA, CRICOS, or other regulators).

5.4 The Institute maintains a log of all records destroyed or archived, and staff are trained to identify records that may require longer retention due to legal, academic, or regulatory significance.

6. Archives

6.1 Records deemed to be of archival value, including those documenting key institutional decisions, strategic initiatives, governance processes, policy development, critical incidents, and legally or historically significant events, must be preserved in a secure and accessible manner for as long as required under relevant legislation or institutional policy.

6.2 Operations is responsible for identifying, classifying, and managing records that require long-term preservation. This includes:

6.2.1 Maintaining a register of archived records.

6.2.2 Applying appropriate metadata for retrieval and audit purposes.

6.2.3 Ensuring that digital archives are migrated to sustainable formats and systems to prevent technological obsolescence.

6.2.4 Archived records must be stored in secure environments that are protected from unauthorised access, deterioration, or damage, and must comply with applicable requirements of the State Records Act 1998 (NSW), Privacy Act 1988, and relevant higher education and research data retention guidelines.

6.2.5 Access to archived records is restricted to authorised staff and may only be granted for legitimate operational, legal, compliance, or research purposes.

6.2.6 Retrievals and access requests must be logged and reviewed by Operations.

6.2.7 Where a record's archival retention period has lapsed and it is no longer required for business, legal, historical, or regulatory purposes, it must be disposed of securely in accordance with the Institute’s approved Retention and Disposal Schedule.

7. Breaches

All members of the Institute should immediately report any suspected or perceived breach of this Policy, Data Protection Policy and Procedures, Critical Incident Policy and Procedures or associated legislation, to their relevant supervisor in the first instance. Breaches will be investigated, and disciplinary action will be taken as appropriate.

8. Academic Records Management

The Institute maintains accurate, current, and secure records of student enrolment, academic progression, course completions, and the conferral of qualifications. These records are:

8.1 Managed by the Registrar in collaboration with academic and administrative units.

8.2 Maintained in secure student management systems with restricted access based on role.

8.3 Retained in accordance with regulatory requirements and the Institute's retention schedule.

8.4 Auditable to ensure the integrity of student outcomes and certification.

8.5 A comprehensive record of each student's academic history, including admission, enrolment status, unit completion, grades, progression decisions, deferrals, and graduation, is maintained for a minimum of 30 years in compliance with the State Records Act 1998 (NSW).

9. Misconduct, Grievances, Complaints, Appeals, and Critical Incident Records

The Institute maintains detailed records to ensure accountability, transparency, and compliance with legal and regulatory requirements. These records capture the full lifecycle of issues, from reporting through to resolution and follow-up.

9.1 **Scope of Records:** The Institute maintains records relating to:

9.1.1 **Formal complaints**: Academic, non-academic, and administrative complaints submitted by students, staff, or external stakeholders.

9.1.2 **Misconduct allegations:** Academic misconduct, research integrity breaches, plagiarism, and any other professional or behavioural misconduct.

9.1.3 **Critical incidents:** Events that pose a threat to the safety, health, or wellbeing of students or staff, or that may significantly disrupt institutional operations.

9.1.4 **Appeals:** Student and staff appeals and the outcome of the appeals process.

9.2 **Documentation Requirements:** Records for each matter must include:

9.2.1 The original complaint, allegation, or incident report.

9.2.2 Documentation of investigations, including evidence collected, witness statements, and analysis.

9.2.3 Actions taken by the Institute, including decisions, sanctions, and recommendations.

9.2.4 All correspondence with affected parties, including notifications, updates, and outcomes.

9.2.5 Details of any appeals, reviews, or subsequent actions, including outcomes and timelines.

9.3 **Security and Access:** Records must be maintained securely in accordance with the Institute’s Information and Privacy Policy and Procedures.

9.3.1 Access is restricted to authorised personnel directly involved in the management or oversight of the matter, such as the Compliance, Registrar, or Student Services staff.

9.3.2 Classification of records will be “Restricted to Staff” or “Strictly Confidential” depending on the sensitivity of the matter, with stricter handling for records involving minors, international students, or critical incidents affecting health and safety.

9.4 **Retention and Compliance:** Records are retained in accordance with the Institute's retention schedule and relevant legislation, including the ESOS Act 2000, the National Code 2018, the Privacy Act 1988 (Cth), and applicable state recordkeeping laws.

9.4.1 Retention ensures the Institute can demonstrate compliance, provide evidence in audits, and respond to any regulatory inquiries.

9.4.2 Where applicable, records relating to international students are retained to support compliance with CRICOS obligations, including reporting to the Department of Home Affairs through PRISMS.

9.5 **Oversight and Monitoring:** The relevant department is responsible for monitoring the completeness, accuracy, and security of records.

9.5.1 Periodic audits of records will be conducted to ensure proper classification, compliance with retention schedules, and adherence to privacy and security standards.

9.5.2 Lessons learned from complaints, misconduct cases, or critical incidents will inform policy updates, staff training, and continuous improvement initiatives.

9.6 **Integration with Student Records:** All relevant records are linked to the student's academic record in the Institute's student management system, where appropriate, to maintain a holistic record of the student's engagement, support, and any interventions applied.

9.6.1 Sensitive information is handled in line with ESOS, the National Code, and the Institute's policies to safeguard the rights and privacy of international students.

10. Data Security and Fraud Prevention

The Institute actively prevents unauthorised or fraudulent access to sensitive information through:

10.1 Role-based access controls to information systems, reviewed annually or when responsibilities change.

10.2 Multi-factor authentication (MFA) and password-protected access to student and staff systems.

10.3 Audit logging of all access and changes to records, with regular audits conducted by Operations.

10.4 Encryption of stored and transmitted personal and academic data.

10.5 Restricted administrative privileges, granted only to authorised personnel trained in data security protocols.

10.6 Any suspected breach or unauthorised access attempt is investigated promptly. Confirmed incidents are escalated as per the Institute's Data Protection Policy and Procedures and, where required, reported to relevant regulatory bodies.

11. Responsibilities

11.1 **Chief Executive Officer:** Overall accountability for compliance with legislative and regulatory obligations.

11.2 **Operations:** Oversight of records management systems, audits, and regulatory reporting.

11.3 **Information Owners:** Accountable for the integrity, access, and retention of records within their area.

11.4 **Staff, Contractors, Board and Committee Members:** Responsible for creating, maintaining, and managing accurate records of Institute business.

11.5 **Educational Agents and Third Parties**: Required to comply with this Policy as a condition of engagement.

Related Legislation

This policy should be read in conjunction with the following related documents:

- Higher Education Standards Framework (Threshold Standards) 2021
- Education Services for Overseas Students Act 2000
- Copyright Act 1968
- Anti-Discrimination Act 1977
- Privacy and Personal Information Protection Act 1988
- Criminal Code Act 1995
- Privacy Amendment (Private Sector) Bill 2000 (Cth)
- Privacy Amendment (Enhancing Privacy Protection) Bill 2021 (Cth)
- Australian Privacy Principles (2014) (Cth)
- Health Records Information and Privacy Regulation (NSW) 2012
- NSW Civil & Administrative Tribunal
- State Records Act (NSW) 1998

Change and Version Control

Version	Date Approved	Authored by	Approved by	Description
1.0	29/09/2023	Chief Executive Officer	Board of Directors	Corporate Policy

Policy Information

Author	Chief Executive Officer

Responsible Officer	Chief Executive Officer
Approved by	Board of Directors
Approval date	29/09/2023
Status	Approved (Current Version)
Next review due	29/09/2027

Name of Policy	Information and Records Management Policy and Procedures	
Version	V1.0	
Policy: Corporate	Date: 29/09/2023	Status: Final ratified by the Board of Directors on 29/09/2023

File: Information and Records Management Policy and Procedures_V1.0

Appendix 1: Privacy Breach Response Procedure

Privacy Breach Response Procedure

Purpose

This procedure outlines the steps to be followed in the event of an actual or suspected privacy breach involving personal, sensitive, or student information, including international student data, to ensure timely containment, mitigation, and reporting in accordance with the Institute's Information and Privacy Policy and Procedures, the ESOS Act 2000, the National Code 2018, and the Privacy Act 1988 (Cth).

Scope

This procedure applies to all staff, contractors, volunteers, and third-party service providers who manage, store, or have access to personal or sensitive information, including student records, staff records, and website-collected data.

Definitions

- Privacy Breach: Any unauthorised access, disclosure, loss, or misuse of personal, sensitive, or student information.
- Sensitive Information: Personal data that, if compromised, could result in harm, including health information, academic records, or financial details.
- Information Owner: The staff member responsible for the security and management of the information or record in question.

1. Detection and Reporting

1.1 All staff must immediately report any actual or suspected privacy breach to their Supervisor and the Information and Records Management Officer.

1.2 Reports must include:

- Nature of the breach (e.g., unauthorised disclosure, data loss, hacking).

- Type and volume of information involved.
- Individuals or groups potentially affected.
- Time and location of the incident.

1.3 If the breach involves international student data, the Operations must also be notified due to potential ESOS compliance implications.

2. Containment and Assessment

2.1 Upon notification, the delegated Information and Records Management Officer will:

- Contain the breach immediately to prevent further unauthorised access or disclosure.
- Secure affected systems, devices, or physical records.
- Suspend access to accounts or files as necessary.

2.2 Conduct a preliminary assessment to determine:

- The severity of the breach.
- The risk of harm to affected individuals.
- Whether the breach involves regulatory obligations under ESOS, the National Code, or other legislative frameworks.

3. Investigation

3.1 A formal investigation will be initiated by the Operations, led by the Information and Records Management Officer.

3.2 The investigation will:

- Identify the root cause of the breach.
- Determine the scope, including which information and which individuals are affected.
- Document all actions taken, findings, and timelines.

3.3 Staff implicated in causing the breach will be interviewed, and any mitigating factors considered.

4. Notification and Communication

4.1 Affected individuals will be notified as soon as practicable, including:

- A description of the breach.
- Potential risks to the individual.
- Steps the Institute has taken or will take to mitigate harm.
- Guidance on protective actions individuals may take.

4.2 For breaches involving international students, Operations will notify the Department of Home Affairs if required under PRISMS or ESOS obligations.

4.3 Internal stakeholders (e.g., Executive Leadership Team, Board) will be informed of breaches according to the severity and risk assessment.

5. Mitigation and Remediation

5.1 Implement immediate measures to mitigate the breach, which may include:

- System patches or updates.
- Restoring data from secure backups.
- Changing access credentials and permissions.
- Staff re-training on data handling and privacy requirements.

5.2 Develop a remediation plan to prevent recurrence, including policy updates, enhanced security measures, and monitoring protocols.

6. Documentation and Recordkeeping

6.1 All privacy breach incidents will be fully documented, including:

- Nature and cause of the breach.

- Affected individuals and information.
- Actions taken to contain and mitigate the breach.
- Communication with affected parties.
- Lessons learned and procedural improvements.

6.2 Documentation will be securely stored in accordance with the Institute’s Information and Records Management Policy and Procedures and classified as “Restricted to Staff” or “Strictly Confidential”.

7. Review and Continuous Improvement

7.1 Following a privacy breach, the Institute will conduct a review to evaluate the effectiveness of the response and identify areas for improvement.

7.2 Recommendations from the review will be implemented to strengthen privacy protections, staff training, and compliance monitoring.