PRIVACY POLICY

1. Purpose

1.1 This document applies to the Innovative Institute of Australia, its courses, its clients (students), and its controlled entities (collectively, "IIA", "Institute", "the Institute", "we", "us", "our"), and to students.

1.2 The purpose of this policy is to

i. Provide the Institute with a policy framework that enables our compliance with the Privacy Act 1988 (Privacy Act) and the Australian Privacy Principles (APPs).

ii. define the approach and circumstances for the collection, use and disclosure of personal information.

iii. Provide strategies to keep information secure, including hard copy and digital information.

iv. Provide a system to classify information that enables the access to, distribution and handling of this information to be controlled.

1.3 This policy is implemented in compliance with the requirements of the Education Services for Overseas Students Act 2000 (the ESOS Act), the Standards for Registered Training Organisations (2025), and the National Code of Practice for Providers of Education and Training to Overseas Students 2018 (the National Code 2018).

1.4 In this file, words that import gender include all other genders; the singular 'they' is gender-neutral and used to avoid specifying a person's gender; words in the singular number include the plural and vice versa.

1.5 This policy does not affect students' rights under the Australian Consumer Law.

1.6 The Institute reserves the right to amend these terms and conditions at any time.

1.7 This policy does not affect students' rights under the *Australian Consumer Law*.

2. Definitions

2.1 Personal information means information or opinions that can identify or reasonably identify an individual, which includes an individual's name, signature, address, phone number, date of birth, employee record information, photographs, internet protocol (IP) addresses, biometric data like voice prints and facial recognition (as they capture unique characteristics of a person), and location data from mobile devices, which can disclose patterns or habits of user activity.

2.2 Sensitive information means personal information or opinions concerning an individual's racial or ethnic origin, political opinions, political association memberships, religious beliefs or affiliations, philosophical beliefs, memberships of professional or trade associations, trade union memberships, sexual preferences or practices, criminal records, health information, genetic information that does not constitute health information, biometric information intended for automated biometric verification or identification, and biometric templates.

2.3 Credit information means specific details collected and used to evaluate an individual's creditworthiness. Credit information includes the full name, date of birth, sex, current or last known address, previous two addresses, current or last known employer's name, driver's licence number, and information about credit providers that have extended consumer credit to a person, including whether they are ASIC-licensed. It also includes details about the type and terms of consumer credit provided, dates of credit availability and termination, credit limits, repayment obligations, repayment history (including timely or missed payments and financial hardship records), and information regarding credit enquiries made by providers in response to a person’s credit applications.

2.4 An education agent refers to an entity (in or outside Australia) that

i. Engages in any of the following activities in relation to a provider:

A. The recruitment of overseas students, or intending overseas students;

B. providing information, advice or assistance to overseas students, or intending overseas students, in relation to enrolment;

C. otherwise dealing with overseas students, or intending overseas students;

and

ii. is not a permanent full-time or part-time officer or employee of the Institute.

2.5 Agent Agreement refers to the agreement between the Institute and the agent, including the schedules.

2.6 CRICOS refers to the Commonwealth Register of Institutions and Courses for Overseas Students.

2.7 ESOS Act refers to the *Education Services for Overseas Students Act 2000 of the Commonwealth of Australia*.

2.8 National Code refers to the *National Code of Practice for Providers of Education and Training to Overseas Students 2018*.

2.9 Prospective student/applicant/client refers to a person who intends to become, or who has taken any steps towards becoming, an 'overseas student' or 'intending overseas student' as defined by the *ESOS Act*.

2.10 DHA refers to the Department of Home Affairs.

2.11 OSHC refers to the Overseas Student Health Cover.

2.12 eCoE refers to the electronic Confirmation of Enrolment.

2.13 2025 Standards for RTOs refers to the *National Vocational Education and Training Regulator (Outcome Standards for NVR Registered Training Organisations) Instrument 2025*.

3. Policy

3.1 The Institute collects and stores personal and sensitive information on our students and industry clients. In doing this, the Institute has introduced this policy to comply with its obligations under the Privacy Act. Protecting personal and sensitive information is essential not only to comply with the Privacy Act but also to safeguard The Institute staff and students from potential financial or reputational harm. Mishandling personal and sensitive data can lead to breaches of trust, significant

reputational damage, and potential loss of enrolments, business partners, and revenue.

3.2 Implementing robust personal and sensitive information security practices offers tangible benefits, including streamlined, efficient processes across the Institute's operations. It substantially reduces the risk of privacy breaches and minimises the resources required to manage and resolve any incidents that may occur. Many of the strategies outlined in this policy will also enhance our ability to handle other sensitive information, such as confidential information, effectively and responsibly.

3.3 Authority to collect and store information

i. The Institute is an approved Registered Training Organisation by the National VET Regulator. This registration is issued under the authority of the National Vocational Education and Training Regulator Act 2011. This legislation requires the Institute to collect personal and sensitive information from our students. This requirement is specified in the Data Provision Requirements 2020, which is one of the legislative instruments that The Institute must comply with as a condition of its registration.

ii. The Data Provision Requirements 2020 (DPR) require the Institute to collect data from students in accordance with the Australian Vocational Education Training Information Statistical Standard (AVETMISS). The DPR is a complex information standard that defines who the student is, where the training is delivered, and what they are studying. The Compliance Standards for RTOs require The Institute to retain and store this information for up to 30 years and to report training activity to government agencies in accordance with mandatory reporting requirements.

iii. In addition to the Data Provision Requirements 2020, the Student Identifiers Act 2014 also requires the Institute to collect high-risk personal information for the purpose of creating or verifying a student's Unique Student Identifier. Together, these requirements constitute a statutory obligation to collect, store, and report information on any student participating in nationally recognised training with

the Institute.

3.4 Use of personal information: To comply with its obligations under the Data Provision Requirements 2020, the Student Identifiers Act 2014, or contractual obligations, or to facilitate an outcome of a service offered to students, The Institute will use personal information to comply with reporting obligations to Government agencies at the Commonwealth level and if accessing Government subsidised training, also with a relevant State or Territory Government agency. Under some circumstances, such as to facilitate an outcome of a service (such as licensing), the Institute may also need to report personal information to other relevant Government or responsible agencies. Students enrolling in a course with The Institute are advised of our collection and use of personal information in the Student Handbook sections on “Your Privacy” and “National VET Data Policy”.

3.5 Solicited information

i. Contact information, such as name, organisation, position, address, telephone, and email, is collected for marketing, support services, mandatory reporting, and communicating with stakeholders as part of our day-to-day operations.

ii. In addition to collecting training activity information, the Institute will also collect, store and report information relating to satisfaction surveys, complaint handling and our client employers.

iii. Names, addresses, phone numbers, emergency contact details, bank account details, and other employment-related information are collected from employees to manage human resources. The management of staff personal information complies with this policy.

3.6 Sensitive information: Personal information collected by The Institute that may be regarded as ‘sensitive’ under the Privacy Act includes

i. 'Disability' and 'long-term impairment status' (health); and 'indigenous status', 'language spoken at home', 'proficiency in spoken English', 'country of birth' (implies ethnic/racial origin). This information is specified in the AVETMISS data elements and is collected for the national VET data collections, national VET

surveys, and may be collected for VET-related research.

ii. 'Dietary requirements' (health-related) are collected for event catering purposes only.

iii. Biographical information, which may contain information on 'affiliations' and 'membership of a professional or trade association', is obtained from keynote speakers for event marketing purposes.

iv. 'Memberships of professional associations' and 'health and work injury information' are collected from The Institute employees for HR management purposes.

3.7 Direct marketing: The Institute respects an individual's right not to receive marketing materials and provides an option in its communications and on its website to unsubscribe. The Institute conducts its marketing communications and dissemination of service information in accordance with Australian Privacy Principle 7 (Direct marketing), the Spam Act 2003 (in respect of electronic communications), and the Do Not Call Register Act 2006. It is not the Institute's practice to 'cold call' to market its products and services. The Institute does not undertake unsolicited marketing practices.

3.8 Unsolicited personal information

i. Unsolicited personal information is information that The Institute may receive without having actively requested it. If the Institute receives unsolicited personal information, it will be treated and managed in accordance with the APPs, which means the Institute will need to assess whether holding it is lawful. If the answer to either of these questions is no, the Institute is to destroy or de-identify the information as soon as practicable and inform the owner of the information of the actions.

ii. The following is a practical example of protecting unsolicited personal information: A parent of a student sends an email to The Institute with records of their young adult son's medical history and condition. The Institute did not request this information and does not require it for any reasonable purpose in

providing services to the student. In this scenario, the Office Manager, with the CE, O, should promptly evaluate the information. This evaluation would determine that the Institute could not have lawfully collected private medical information; it must securely destroy or de-identify the information as soon as possible and advise the parent and student of this action.

3.9 Notification of collection: The Institute aims to notify individuals of the collection of their personal information before, at the time of, or as quickly as possible after collection. Notifications are usually in writing, but may be verbal over the phone. Examples of notification include:

i. Marketing - notification is provided on our website's course application page. Individuals are also notified when personal information is collected for events. A privacy notice is provided in all The Institute marketing communications.

ii. Pre-enrolment information supplied to the prospective student before their enrolment or commencement includes the Student Handbook. Students enrolling in a course with The Institute are advised of our collection and use of personal information in the Student Handbook sections on "Your Privacy" and "National VET Data Policy".

iii. Quality Indicator surveys: notification is provided in the invitation email to participate in the surveys, and again when the information is collected.

iv. The Institute staff: Notification is provided upon employment commencement.

3.10 Disclosure of personal information

i. The Institute is not to disclose personal information other than for the purpose for which it was collected, or an individual has consented to a secondary purpose, or an individual would reasonably expect this (such as receiving communications about upcoming events), or if required by law.

ii. The Institute may share personal information with the Commonwealth government in accordance with Commonwealth contractual or regulatory obligations. In these circumstances, the Institute will take reasonable steps to

inform and seek consent from the individuals concerned, and to ensure that the recipient handles the personal information in accordance with the APPs.

iii. The Institute is not to sell or distribute mailing lists or student contact information to third parties under any circumstances. The Institute does not disclose personal information to overseas recipients. While people around the world can access material published on our website, no publications on our website are to contain identifiable personal information.

3.11 Management of personal information: The Institute will ensure that the personal information it collects, uses, or discloses is accurate, up-to-date, complete, and relevant. The Institute routinely updates the information held in its student management system, including confirming with returning students whether their personal contact details have changed.

3.12 Access to and correction of personal information

i. Individuals may, subject to the exceptions prescribed by the APPs, request access to and correction of their personal information where this is collected directly from individuals by The Institute.

ii. The Institute does not charge for granting access to or correcting personal information, unless the student requests copies of information, which may incur an administrative fee.

3.13 Retention and recording of high-risk personal information

i. In accordance with the APPs principles 11.2 and the Student Identifiers Act 2014, section 11, the Institute is not to continue to hold information where it has no further purpose for this information. An example of this may include high-risk personal information, such as a copy of a student's passport, driver's licence, or Medicare Card. Once the student's identification or eligibility has been verified (the purpose), the Institute will destroy these records by shredding or permanently deleting them so that they are no longer stored. The Institute's information security risk is significantly reduced if these records are destroyed as soon as possible once the purpose for collecting this information is satisfied.

ii. Where possible, staff should seek to verify high-risk personal information directly with the student, either in person or via video conference, to avoid the need to collect and store these records altogether.

iii. The Institute is to retain the details of high-risk personal information used for verification by recording the type of information viewed, the date it was viewed, and by whom.

3.14 Information security: The Institute is to apply strict security controls over the information it has collected and stores, including hard copy and digital records. The following guidelines are provided for the handling and storage of both hard copy and digital records:

i. Hard copy information security. All the IInstitute'shard copy information is to be stored to prevent unauthorised access. This includes unauthorised access by staff members who have no legitimate purpose for accessing the information to perform their duties. Where possible, the storage of hard-copy information is to be minimised, with preference given to digitising records that need to be retained. The following strategies are to be applied to the storage and handling of hard copy information:

A. Secure storage. Sensitive information must always be stored securely in locked cabinets or rooms accessible only to authorised personnel.

B. Controlled access. Distribution of keys or access codes for locked areas must be limited exclusively to authorised staff, with clear records maintained of all keyholders.

C. File organisation and labelling. All information and files are to be clearly labelled and organised consistently to facilitate effective storage and retrieval, while ensuring security and confidentiality.

D. Secure disposal. Outdated or unnecessary sensitive information must be disposed of securely, utilising methods such as shredding to prevent unauthorised access.

E. Staff training. New and existing staff are to be trained in proper handling,

storage, labelling, and confidentiality procedures for hard copy information.

F. Office security measures. Office doors, particularly those leading to areas housing sensitive information, must remain locked whenever unattended or outside of working hours.

G. Visitor management. Visitors must be escorted at all times when accessing areas where sensitive records are stored, ensuring continuous monitoring of access to these records.

H. Regular access audits. Monthly audits are be conducted to verify and update authorisation records for keys and access codes, ensuring access remains restricted and up-to-date.

I. Digitisation and backup. Critical information should be digitised as appropriate, with electronic copies securely stored and backed up regularly to provide additional protection against loss or damage.

J. Clean desk policy. Staff must adhere to a clean desk policy, ensuring that all sensitive files and information are properly secured at the end of each working day.

ii. Digital information security. The following strategies are to be applied to the storage and handling of digital information:

A. Cybersecurity responsibilities. The CEO, with the support of the Office Manager, is responsible for overseeing information security awareness and compliance.

B. User access management. User access to systems and cloud services must be strictly controlled. All users are required to use unique credentials, maintain strong passwords, update these regularly, and enable multi-factor authentication (MFA) wherever it is available.

C. Cloud service security. The Institute authorises the use of trusted cloud-based providers, such as Microsoft 365, Dropbox, Google Drive, or similar services. Permissions for accessing stored data are to be set according to

roles and regularly reviewed to ensure appropriate data access.

D. Device security. All devices, such as computers, printers, routers, etc., must have automatic device drivers and security updates enabled and regularly maintained. Reliable antivirus software (such as Norton's) must be installed, configured for daily scanning, and kept up to date, along with an active firewall to prevent unauthorised network access.

E. Data encryption and backup. Sensitive information stored or transmitted by The Institute must be encrypted to ensure privacy and confidentiality. This includes data stored within student management systems. The Institute must verify with third-party suppliers of student and learning management systems that the Institute's data stored in these systems is protected by encryption both in transit and at rest. Data backups must be performed regularly and securely stored in cloud services or off-site locations. The Institute must verify the ability of third-party suppliers of student and learning management systems to recover and restore services to a restore point that must not exceed 24 hours.

F. Remote work security. Personnel must follow clearly defined guidelines to work remotely securely. This includes the secure use of collaboration and communication platforms such as Teams or Zoom, and the avoidance of public Wi-Fi networks unless securely connected via VPN.

G. Staff cybersecurity training. All staff are to undertake annual privacy and information security training to maintain their understanding of cybersecurity threats and best practices, including recognising phishing attempts, safe password management, and appropriate handling of sensitive information.

H. Email security. The Institute's email systems are to include active spam filtering, phishing protection, and multi-factor authentication. Staff must use official organisational email accounts for all work communications, and exercise caution with email attachments and links. All email correspondence sent or received using official organisational email

accounts remains the property of The Institute.

I. Website security. The Institute's website will maintain secure hosting with active SSL certification. The website and all plugins, themes, and extensions must be updated regularly. Security plugins or firewall tools (such as Wordfence) must be implemented to detect, prevent, and alert administrators to potential threats and block unwanted traffic.

J. Website access controls. Website administrative access for The Institute must be limited strictly to authorised personnel, who must use secure passwords and MFA. Regular website backups must be securely maintained, and unnecessary files or outdated user accounts must be routinely removed to mitigate risks.

3.15 Information classification labels

i. The Institute is to use information classification labels to clearly identify the sensitivity and importance of the information handled by staff, students, and partners. Information classification labels guide staff on how to appropriately handle, store, and share information, thereby reducing risks associated with unauthorised disclosure, misuse, or loss. Labels support compliance with legal and regulatory obligations, helping The Institute avoid potential penalties and safeguard our reputation. Additionally, clear labelling of information promotes consistent information security practices across our operations, reinforcing staff accountability and awareness.

ii. The table below explains the eight information classification labels to be used at The Institute. These labels are not listed in any hierarchy or sequence of importance. Each label is fit for its intended description. The CEO, with the support of the Office Manager, will allocate information classification labels where these are not already identified below as examples. The colour shown in the table below must be used to highlight the classification, with the Internal classification being displayed as Blue and others, including Confidential, Restricted, Private and Critical,l displayed in Red. Some information classifications do not require display.

iii. Information classification labels must be prominently displayed on each item of information where practical, and the need to display the classification is specified in the Information classification label rules outlined in the table below.

Label	Description	Examples	Rules
Public	Information intended for public access, openly available internally and externally without restrictions.	Marketing brochures Website content Student Handbook	No special security measures required. May be shared externally without approval.
Internal Only	Information available only to The Institute employees or approved partners and not intended for public dissemination.	Policies and procedures Meeting minutes Internal correspondence Continuous improvement records	Distribute internally or to authorised partners only. Not for public disclosure without approval. Must be displayed on the information.
Academic	Information created specifically for training, learning, or assessment purposes within or associated with The Institute.	Training manuals Course handbooks Assessment guidelines and resources Student workbooks and learning activities Training and assessment strategies	Distribute to students and trainers. May be shared externally with authorisation. Not intended for unrestricted public dissemination unless explicitly approved.
Confidential	Information that, if disclosed externally, could negatively impact business operations, reputation, or competitive advantage.	Business plan Financial performance information Contractual agreements	Limit access to a need-to-know basis. Secure storage and handling required. External sharing needs explicit authorisation. Must be displayed on the information.

Label	Description	Examples	Rules
Restricted	Highly sensitive business information that could lead to serious financial, legal, or reputational damage if improperly disclosed.	Legal advice or litigation information Critical intellectual property Business sale information	Access restricted to explicitly approved personnel. Secure encryption is required using BitLocker No external sharing without CEO authorisation. Must be displayed on the information.
Private	Privacy laws and internal policies protect personal or sensitive information about staff or students.	Student's personal information Staff personal information Payroll information Student or employer payment details	Compliance with privacy laws. Restricted access is only to those who need access to perform their duties. Secure storage, transmission, and disposal required. Must be displayed on the information.
Critical	Information vital for the ongoing operations, continuity, and stability of the business. Its loss or compromise could severely impact operations.	Business continuity plans Critical infrastructure documentation Insurance records Administrator security credentials	Secure storage with regular backups. Limited access to authorised personnel. Regular integrity checks/audits. Must be displayed on the information.
Regulatory	Information required by law, regulations, industry standards, or compliance	Records that show compliance with standards	Comply fully with relevant regulations. Regular audits and

Label	Description	Examples	Rules
	frameworks. Disclosure, handling, or storage governed externally.	Financial viability information Work health and safety records	monitoring. Clear recordkeeping and accountability are required.

VERSION HISTORY

Version Number	Date	Summary of changes
1.0	September 2021	New policy
2.0	July 2025	Revised and updated to include the changes according to the Standards for Registered Training Organisations (2025).
3.0	December 2025	Revised and updated to include the changes according to the ESOS 2000 Act.