Privacy and Data Use Policy and Procedure

1. Purpose

The purpose of this Policy and Procedure is to ensure the confidentiality, security and proper handling of students', staff and stakeholder personal data ensuring the protection of individual privacy at the Australian College of Business Intelligence (ACBI/the College).

These measures align with the Privacy Act 1988, incorporating the Australian Privacy Principles (APPs) and the amendments made by the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

2. Rationale

The *Privacy and Data Use Policy & Procedure* is a critical component of ACBI's governance and compliance framework. It ensures that the collection, storage, use, and disclosure of personal information complies with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Student Identifiers Act 2014, and relevant VET sector legislation including the National Vocational Education and Training Regulator Act 2011.

ACBI is entrusted with the personal and sensitive information of students, staff, contractors, and stakeholders. The integrity and security of this information is fundamental to maintaining the trust of these individuals and meeting our statutory obligations. The consequences of mishandling personal information include not only reputational damage and legal liability but also potential disruption to operations and student outcomes.

This Policy and Procedure provides a clear, structured approach to privacy protection by setting out guiding principles, responsibilities, and processes for the lawful and secure management of personal information. It reflects a commitment to best practice in data protection, risk management, and digital security, ensuring that information is handled with the utmost care and in accordance with evolving regulatory expectations under the Standards for RTOs 2025.

By embedding privacy protections in daily operations, this policy contributes to the ethical and compliant delivery of training services and supports our broader objectives of quality assurance, transparency, and student-centred practice.

3. Policy

ACBI is committed to protecting the privacy and security of personal information and to upholding the rights of individuals. This Privacy and Data Use Policy and Procedure ensures that personal information is handled lawfully, securely, and transparently in accordance with relevant legislation and regulatory standards.

ACBI manages all personal information in compliance with the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs), and the Privacy Amendment (Enhancing Privacy Protection) Act 2012. This policy also aligns with the Standards for Registered Training Organisations 2025, the National Vocational Education and Training Regulator Act 2011 (Cth) (NVETR Act), the Student Identifiers Act 2014, and the Data Provision Requirements 2020.

In accordance with the NVETR Act, ACBI is obligated to disclose personal information collected from students to the National VET Data Collection, managed by the National Centre for Vocational Education Research Ltd (NCVER), and, where applicable, to the relevant state or territory training authority.

ACBI also complies with the Data Provision Requirements 2020, which mandate the collection, verification, and submission of accurate AVETMISS data to NCVER for national VET policy and planning purposes. All data collected under these provisions is managed securely and in alignment with the Privacy Act 1988 and the APPs.

All students undertaking nationally recognised training are required to have a Unique Student Identifier (USI). Students must provide their USI at enrolment, or ACBI may apply for a USI on their behalf. The Student Identifiers Act 2014 authorises the Australian Government's Student Identifiers Registrar to collect personal information to create and manage USIs.

When applying for a USI on a student's behalf, ACBI must collect and provide the minimum following personal information to enable Student Support to generate the USI:

- Name (including given name(s), middle name(s), and family name)
- Date of birth
- City or town of birth
- Country of birth
- Gender
- Contact details

Where a student does not provide the required information, Student Support will be unable to issue a USI, and ACBI will not be able to issue a qualification or statement of attainment.

4. Scope

This policy applies to all employees, students, contractors, and other individuals associated with ACBI who are involved in the collection, use, and disclosure of personal information.

This policy applies to all students enrolled with ACBI, including both domestic students and international students studying in Australia on a student visa (CRICOS students).

It is intended to ensure consistent application of the RTO's responsibilities under the Standards for RTOs 2025 and, where applicable, the Education Services for Overseas Students Act 2000 and the National Code of Practice for Providers of Education and Training to Overseas Students 2018.

Where obligations differ for CRICOS students, specific provisions are identified at the end the policy and procedure.

5. Definitions

Personal Information defined under the Privacy Act 1988 (Cth) refers to any information or opinion about an individual, or that may reasonably identify an individual.

Privacy Act 1988 refers to an Australian law which regulates the handling of personal information about individuals.

Australian Privacy Principles (APPs) are contained in the Privacy Act 1988 and outline the handling, use and management of personal information.

Consent, as defined in s 6(1) of the Privacy Act 1988 (Cth), refers to 'express consent or implied consent'. The four key elements of consent include the individual being adequately informed before giving consent, the individual giving consent voluntarily, the consent is current and specific, and the individual has the capacity to understand and communicate their consent.

6. Responsibility

The **CEO** is responsible for implementing and monitoring the Privacy and Data Use Policy and Procedures and for addressing any queries or concerns about privacy matters.

The **CEO** and **Facilities Coordinator**, supported by ACBI's external IT provider, oversee cybersecurity compliance.

7. Requirements

The College must act in accord with the requirements of the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs) and the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

Data Provision Requirements 2020 (legislative instrument made under section 187 of the National Vocational Education and Training Regulator Act 2011).

Education Services for Overseas Students Act 2000 (ESOS Act), National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code).

ACBI must also comply with the Standards for Registered Training Organisations (RTOs) 2025 - Standard 4.4 (2) (c) - it has mechanisms in place to lawfully collect and analyse data including any feedback received from VET students, staff, industry, VET regulators, State and Territory training authorities and employers of current or former VET students.

8. Procedure

ACBI ensures the lawful, fair, and secure handling of personal information throughout its lifecycle. Personal information is collected directly from students, staff, or stakeholders through application forms, consent forms, request forms (e.g. forms relating to enrolment variations) and correspondence.

Information collected is limited to what is reasonably necessary for training delivery, compliance, reporting, and student support. ACBI notifies individuals at or before the time of collection through the Enrolment Acceptance Agreement and privacy statements available on the website, and seeks informed consent where required. Once collected, this information is used to support training delivery, reporting, and compliance functions in accordance with privacy laws.

Once collected, personal information is used for enrolment processing, student management, support services, training delivery, compliance with reporting requirements, and issuing qualifications. Use and disclosure are limited to the primary purpose of collection or a directly related secondary purpose where consent is provided or legally required. Disclosure may be made to NCVER, the USI Registrar, government agencies, and authorised third parties for regulatory, statistical, and funding purposes.

All personal information is stored securely, either digitally within password-protected systems or physically in locked storage. ACBI uses encryption, access controls, and antivirus software to protect digital data. ACBI's chosen Student Management System (RTO Manager by Meshed Group) uses secure infrastructure, including SSL encryption and restricted, authenticated access to protect all data. Information classification labels guide staff on handling sensitive data when uploaded to the Student Management System, such as those marked Confidential.

Students have the right to request access to or correction of their information. Requests are responded to within 10 business days. If personal information becomes unnecessary for any purpose, it is securely destroyed or de-identified.

In accordance with Standard 4.4(2)(c) of the Standards for RTOs 2025, ACBI collects feedback from students, staff, industry, regulators, training authorities, and employers of current or former students to inform continuous improvement. This feedback may include personal or sensitive information. ACBI ensures that all such feedback is handled in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

Feedback is stored securely, access is limited to authorised personnel, and it is only used for the purpose for which it was collected, such as quality assurance and reporting. Identifiable data is de-identified where possible, and feedback mechanisms are subject to regular review as part of ACBI's self-assurance practices.

If ACBI receives unsolicited personal information it is assessed and, if not required, securely destroyed. Any marketing communication complies with APP 7 and allows individuals to opt-out.

Privacy-related complaints can be submitted to the CEO and/or the Compliance Manager. Complaints are handled under the Student Complaints and Appeals Policy and may be escalated to the Office of the Australian Information Commissioner (OAIC) if unresolved.

Privacy compliance is reviewed regularly by the CEO and Compliance Manager and where potential data breaches have occurred, such incidents will be recorded on the Critical Incident Register for tracking from the time the incident is reported to resolution. Recommendations for improvements will be recorded in the Continuous Improvement Register.

Procedure table

Step	Action	Controls	Responsibility
1. Collection of Personal Information	Collect information directly from students, staff, and stakeholders via forms and correspondence	Only collect information necessary for training delivery, compliance, reporting, and support	Admissions team/Student Support
2. Notification & Consent	Inform applicants/students at or before collection through enrolment acceptance agreements and privacy statements	Ensure transparency and obtain informed consent where required	Admissions team
3. Use of Information	Use information for enrolment, training delivery, student support, reporting, and issuing qualifications	Use limited to primary purpose or related secondary purpose with consent or legal authority	Student Support and Operations staff
4. Disclosure of Information	Share data with authorised entities (e.g. NCVER, USI Registrar, government agencies)	Disclosure only for regulatory, statistical, or funding purposes in line with legal requirements	Compliance Manager
5. Storage & Security	Store data securely (digital and physical formats)	Apply encryption, MFA, access controls, antivirus protection, secure backups, and classification labels	All staff handling data and SMS and LMS platform providers
6. Access, Correction, Retention and Disposal	Respond to requests for access or correction of personal information and only retain data as long as necessary	Requests processed within 10 business days and securely destroy or de-identify when no longer required	All staff handling data
7. Marketing Communications	Send marketing communications only where compliant	Provide opt-out options in line with APP 7	Marketing
8. Complaints Handling	Manage privacy complaints through formal process	Escalate unresolved issues to OAIC if required	CEO / Compliance Manager
9. Monitoring & Review	Conduct regular privacy compliance reviews	Record data breaches and improvements in registers	CEO / Compliance Manager

9. Policy Implementation

This policy will be made available to all staff members and stakeholders through the internal communication channels, the website and in the Student Handbook.

All staff receive annual cybersecurity training including identifying phishing, secure password handling, and digital confidentiality.

10. Review and Continuous Improvement

Privacy compliance issues are a standing agenda item at biannual Governance and Risk Committee meetings. Feedback from staff and students is collated, reviewed, and addressed via the Continuous Improvement Register.

This Policy and Procedure will undergo an biennial review, or sooner if required, to ensure it remains relevant and effective in guiding the operations and strategies or as needed to reflect any changes in the regulatory environment or operational practices.

Feedback will be collated and analysed for noting or action with any necessary changes documented in the Continuous Improvement Register.

Document Control

Version number:	2.0	Approved by:	Fabio Mejia (CEO)
Approval date:	13/05/2026	Review date:	13/05/2028
Standards/Legislation: SRTOs 2025 (4.4 [2c]), Privacy Act 1988, Privacy Amendment (Enhancing Privacy Protection) Act 2012, Student Identifiers Act 2014, National Vocational Education and Training Regulator Act 2011, Data Provision Requirements 2020			

Version History:

Version	Date	Author	Reason	Sections
1.0	-	-	Privacy Policy published as dedicated section of the website.	All
2.0	13/05/2026	Sam Hartley	Creation of new policy and accompanying procedure and name changed to include ‘and Data Use” to better reflect the content	All

CRICOS Addendum

Purpose

This CRICOS Addendum outlines the specific requirements relating to the handling of personal information for overseas students, as prescribed by the *National Code of Practice for Providers of Education and Training to Overseas Students 2018*. It ensures that the provider discloses and manages personal information in accordance with its responsibilities under the Code.

ACBI informs overseas students that their personal information may be made available to the Australian Government and designated authorities including the Tuition Protection Service (TPS), the Department of Education, the Department of Home Affairs, and other agencies authorised by law. This information may include details relating to course progress, visa status, and payment records.

Applicable National Code Standard (3.3.6)

CRICOS-Specific Obligations

1. Enrolment Acceptance Agreement Must Include a Disclosure Statement

The provider must ensure that the written agreement (Enrolment Acceptance Agreement) with the overseas student includes a clear statement that:

"Personal information about the student may be shared between the registered provider and the Australian Government and designated authorities and, if relevant, the Tuition Protection Service (TPS) and the TPS Director."

This disclosure applies to:

- Personal and contact details
- Course enrolment details and changes
- Circumstances of any breach of student visa conditions

2. Informing Students Prior to Enrolment

The provider must ensure that this information is:

- Clearly explained in the written agreement
- Provided before enrolment is finalised

3. Application to TPS and Visa Breach Reporting

Disclosures may occur to meet legal obligations related to:

- Tuition assurance through the TPS framework
- Reporting student course variations or suspected breaches of visa conditions

Recordkeeping Requirements

- A copy of the written agreement signed by the student including the disclosure clause
- Procedures to log and track disclosures made to external bodies (where relevant)
- Internal controls to ensure information is only shared in accordance with this requirement
- Evidence that students were advised prior to or at the time of signing the agreement

CRICOS Policy Suite

This Addendum should be read in conjunction with:

- Admissions Policy & Procedure
- Letter of Offer and Enrolment Acceptance Agreement (CRICOS students)
- Student Complaints and Appeals Policy