EVANTAA INSTITUTE

CONDUCT & WELLBEING

Privacy & Confidentiality

Policy & Procedure

How we collect, use, store and protect your personal information.

VERSION	EFFECTIVE	PROVIDER
3.0	June 2026	RTO 45866 · CRICOS 04025C

1. Purpose

The purpose of this policy is to ensure that Evantaa Institute manages personal information in compliance with the Privacy Act 1988 (Commonwealth), the Australian Privacy Principles, the Standards for Registered Training Organisations (RTOs) and the Compliance Requirements. This policy outlines the procedures for collecting, storing, using, and disclosing personal information and ensures the protection of privacy rights for students, staff, and other stakeholders.

2. Scope

This policy forms part of Evantaa Institute's Quality Management System and applies to all students, prospective students, staff, third-party service providers, employers, and all business operations related to the collection, storage, use, and disclosure of personal information.

3. Policy

- Evantaa Institute is committed to protecting personal information and privacy rights in accordance with the Privacy Act 1988, the Australian Privacy Principles, and the Standards for Registered Training Organisations (RTOs) and the Compliance Requirements. We ensure that all personal information collected, stored, used, and disclosed is handled with the highest level of integrity and confidentiality. Personal information will be collected and used with the consent of the individual, unless otherwise required or authorised by law.

Information collected will be used only for the purpose for which it was collected, such as enrolment, student administration, communication, and compliance with regulatory requirements. Where sensitive information is collected, it will only be collected where necessary and with explicit consent from the individual.

Information will be provided to all such government agencies and/or organisations so authorised to receive such information, where the provision of this information is necessary for Evantaa Institute to continue to operate as a registered training organisation and for registration and re-registration purposes.

Personal information will be securely stored, with access restricted to authorised personnel only to protect information from misuse, loss, unauthorised access, modification or disclosure, including restricted access to electronic files, secure storage of paper files and backup of data.

- Evantaa Institute will not disclose information about students to a third party, such as an employer, without written permission from the student.

4. Procedures

A. Collection of Personal Information

- Administration staff must collect personal information during the enrolment process, including student names, contact details, payment details and other information required for admission, training delivery and compliance purposes.
- Administration staff must maintain accurate student records, including personal information, assessment outcomes, transcripts, file notes and related documentation within the Student Management System and student files.
- Staff may collect personal information through normal communication and business activities, including emails, phone calls, meetings and interactions with students or stakeholders.
- IT staff may collect limited website interaction information, including IP address, browser type and accessed pages, where applicable, to support system administration, security and service improvement.

B. Use and Disclosure of Personal Information

- Staff must use personal information only for the purpose for which it was collected or for directly related purposes, including enrolment, training and assessment, student support, communication, compliance and stakeholder engagement.
- Administration staff must ensure that personal information is disclosed to external parties only where consent has been provided, disclosure is required by law, or disclosure is necessary to manage safety, regulatory or operational obligations.
- Staff involved in marketing or communications must ensure that personal information used for communication or promotional activities includes an appropriate opt-out option where applicable.
- Staff must ensure that personal information is not disclosed, shared or accessed without appropriate authorisation.

C. Data Quality and Accuracy

- Administration staff must take reasonable steps to ensure that all personal information collected and maintained by Evantaa Institute is accurate, complete, current and relevant.
- Staff must promptly update records where students or stakeholders provide revised or corrected information.
- Administration staff and IT staff must ensure that personal information is protected from misuse, interference, loss, unauthorised access, modification or disclosure.
- Staff must ensure that records maintained within the Student Management System and physical files are regularly reviewed for accuracy and completeness.

D. Data Security and Storage

- IT staff must implement and maintain appropriate security measures, including password protection, secure systems, restricted access controls and data protection measures to safeguard personal information.
- Administration staff must ensure that access to personal information is limited to authorised staff based on their role and responsibilities.
- Staff must ensure that student information stored within the Student Management System and physical records is securely maintained and accessed only where authorised.
- IT staff must ensure that all online systems, transactions and electronic storage methods comply with appropriate security and industry standards.
- Staff must immediately report any suspected unauthorised access, loss or security concerns relating to personal information to the RTO Manager or Chief Executive Officer.

E. Access to and Correction of Personal Information

- Administration staff must allow students and relevant individuals to request access to their personal information in accordance with applicable privacy requirements.
- Administration staff must verify the identity of the individual prior to providing access to personal information or records.
- Administration staff must provide access to requested information within fourteen (14) days where practicable or notify the individual in writing where access cannot be granted, including the reasons for refusal where applicable.
- Staff must allow individuals to request corrections to personal information and must update records where valid supporting evidence is provided.
- Evantaa Institute will not charge fees for requests relating to access or correction of personal information.

F. Retention and Disposal of Information

- Administration staff must retain personal information and records only for as long as required under applicable legislative, regulatory and operational requirements.
- Staff must ensure that records are securely stored and disposed of appropriately once retention requirements have been met.
- IT staff must ensure that electronic records scheduled for deletion or disposal are securely removed to prevent unauthorised recovery or access.

G. Data Breaches and Notifiable Data Breaches

- Staff must immediately report any actual or suspected data breach, unauthorised disclosure, loss or misuse of personal information to the RTO Manager or Chief Executive Officer upon identification.
- The RTO Manager or CEO must assess any suspected data breach to determine the nature, scope and potential impact of the breach, including whether the breach is likely to result in serious harm.

- Evantaa Institute must manage data breaches in accordance with the Notifiable Data Breaches Scheme and any applicable legislative obligations.
- Where required, the RTO Manager or CEO must ensure that affected individuals and the Office of the Australian Information Commissioner (OAIC) are notified within required timeframes.
- Notifications relating to data breaches must include details of the nature of the breach, the information affected, likely consequences and recommended actions for affected individuals.
- The RTO Manager or CEO must ensure that breach notifications are submitted using the OAIC Notifiable Data Breach process where applicable.
- Staff must document all data breaches, investigations, corrective actions and outcomes and record these within relevant organisational registers and continuous improvement processes.

5. Variations

Evantaa Institute reserves the right to modify this policy as necessary to comply with legislative changes or organisational needs.

Document Control

Document Title	Privacy Confidentiality Policy and Procedure
Version	3.0 (Rebranded and reissued under Evantaa Institute)
Former Version	2.0
Effective Date	15 June 2026
Approved By	Chief Executive Officer (CEO)