PRIVACY POLICY

And Associated Procedures

National Engineering & Construction Training Academy
CRICOS No. 04182A | RTO Code. 46048
www.necta.edu.au

Document Details	
Document Code	NECTA-GOV-PRV-001
Version	V4.0
Effective Date	14 April 2026
Approved By	PEO
Review Date	On or before 14 Apr 2027
Status	Approved
Regulatory Alignment	Privacy Act 1988 | Australian Privacy Principles | NDB Scheme | ESOS Act 2000 | National Code 2018 | Standards for RTOs 2015

Purpose of the Policy

This policy and associated procedures outline Xavier International College Pty Ltd, trading as, National Engineering and Construction Training Academy (NECTA)'s approach to ensuring the privacy and confidentiality of all of its staff, students and relevant others.

This policy and associated procedures meet the requirements of information management of Standard 4.3 of the Outcome Standards for RTOs and Compliance Requirements (Section 1) regarding information management, as well as Standard 3 of the National Code of Practice for Providers of Education and Training to Overseas Students 2018, as well as the National VET Regulator (Data Provision Requirements) Instrument 2020 and National VET Data Policy.

Privacy Legislation and Principles

NECTA is committed to protecting the privacy of personal information and complies with the Australian Privacy Principles contained in the Privacy Act 1988. NECTA ensures that all personal information is collected in a lawful and fair manner, is used only for authorised purposes, and is stored securely to prevent misuse, loss or unauthorised access. NECTA also ensures that individuals are able to access their personal information and request corrections where necessary.

Key Legislative Framework
• Privacy Act 1988 (Cth) — Australian Privacy Principles (APPs)
• Standard 4.3 — Outcome Standards for RTOs and Compliance Requirements (Section 1)
• Standard 3 — National Code of Practice for Providers of Education and Training to Overseas Students 2018
• National VET Regulator (Data Provision Requirements) Instrument 2020
• National VET Data Policy
• ESOS Act 2000 — international student reporting obligations
• Notifiable Data Breaches (NDB) Scheme — Office of the Australian Information Commissioner (OAIC)

Collection of Personal Information

NECTA collects personal information that is reasonably necessary for the conduct of its business operations, including the delivery of training and assessment, provision of student support services, and compliance with regulatory obligations.

Types of Personal Information Collected

The types of personal information collected may include an individual's name, date of birth, contact details, passport details, Unique Student Identifier (USI), educational background, employment history, enrolment details and academic records. In some cases, NECTA may also collect sensitive information such as health information, police checks or working with children checks where this is required for training, employment or work placement purposes.

Collection Methods

Personal information is collected through enrolment forms, student management systems, application processes and direct communication with individuals. NECTA ensures that all personal information is collected by lawful and fair means and that individuals are informed about the purpose of collection at the time the information is obtained.

Collection Method	Information Collected
Enrolment Forms	Name, DOB, contact details, passport details, USI, educational background
Student Management System	Enrolment details, academic records, course progress, attendance
Application Processes	Employment history, qualifications, visa status, agent referral details
Direct Communication	Welfare information, complaints, access and correction requests
Health / Pre-placement Checks	Health information, police checks, Working with Children Checks (where required)

Use of Personal Information

NECTA uses personal information for purposes directly related to its operations. This includes delivering training and assessment services, providing academic and support services to students, issuing AQF certification documentation, maintaining accurate academic and administrative records, and meeting its legal and regulatory obligations.

NECTA may also use personal information to improve its services, respond to enquiries, conduct internal reviews, and communicate important information to students and stakeholders.

Authorised Purposes

- Delivery of training and assessment services
- Provision of academic and student support services
- Issuance of AQF certification documentation
- Maintenance of accurate academic and administrative records
- Meeting legal and regulatory obligations including ASQA, DHA, NCVER and TPS reporting
- Improving services and responding to student and stakeholder enquiries
- Conducting internal reviews and quality assurance activities
- Communicating important information to students, staff and stakeholders

Disclosure of Personal Information

NECTA may disclose personal information where it is necessary to meet regulatory, operational or legal requirements. Personal information may be disclosed to relevant government agencies and regulators, including ASQA, the Department of Home Affairs, and the Tuition Protection Service, and other authorised bodies.

Regulatory Reporting

NECTA is required to report training activity data to the NCVER in accordance with AVETMISS requirements. For international students, personal information is also disclosed through PRISMS for the purposes of managing enrolment, course progress and visa compliance.

Third Party Disclosure

Personal information may also be shared with third parties such as education agents, industry placement providers, contractors and service providers, including those providing student management systems, learning management systems or IT support services. NECTA takes reasonable steps to ensure that these third parties handle personal information in accordance with applicable privacy laws.

ESOS Act and National Code Obligations

NECTA complies with all requirements under the ESOS Act and National Code. This includes reporting enrolment details, course variations, progress and completion through PRISMS. NECTA also maintains up-to-date contact details for all international students and reports any breaches of student visa conditions where required by law. Personal information may be shared with relevant government agencies to support visa monitoring and compliance activities.

Unique Student Identifier (USI)

NECTA is required to collect and verify a valid Unique Student Identifier (USI) for all students undertaking nationally recognised training. A USI must be verified before AQF certification documentation can be issued. NECTA ensures that USI information is stored securely and access is restricted to authorised personnel only. Students are also provided with information about how their USI data will be handled in accordance with privacy requirements.

Recipient	Purpose of Disclosure
ASQA	Regulatory compliance, audit and registration obligations
Department of Home Affairs (DHA)	International student visa monitoring and PRISMS reporting
Tuition Protection Service (TPS)	Student fee protection and course assurance reporting
NCVER	AVETMISS training activity data reporting
Education Agents	Student recruitment and enrolment support (under agency agreement)
Industry Placement Providers	Work placement coordination and student compliance
IT / LMS / SMS Providers	System operation and support (bound by privacy obligations)
OAIC	Notifiable data breach reporting (where applicable)

Sensitive Information

Sensitive information is collected only where it is necessary and directly relevant to NECTA's operations. This type of information is handled with a higher level of care and is used only for the primary purpose for which it was collected, or for a directly related secondary purpose. Sensitive information may also be used or disclosed where required or authorised by law or where consent has been obtained from the individual.

Definition of Sensitive Information

Sensitive information is defined in the Privacy Act to include information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information.

Sensitive Information — Handling Requirements
• Collected only with explicit consent or where required by law
• Used only for the primary purpose of collection or a directly related secondary purpose
• Stored with enhanced security controls and restricted access
• Disclosed only to authorised personnel or bodies with a lawful basis
• Not used for marketing, profiling or any unrelated purpose

Data Storage and Security

NECTA takes all reasonable steps to ensure that personal information is stored securely and protected from misuse, interference, loss, unauthorised access, modification or disclosure. Personal information is stored in secure student management systems and electronic databases that are protected by passwords and role-based access controls. Physical records are stored in secure locations with restricted access.

Staff are trained in the appropriate handling of personal information and are required to follow internal procedures to ensure data security at all times.

Security Controls

- Role-based access controls to all student management and administrative systems
- Password-protected electronic databases and document management systems
- Secure physical storage with restricted access for paper-based records
- Staff training in privacy and data security obligations
- Periodic review of access permissions and system security settings
- Third-party service providers assessed for privacy law compliance prior to engagement

Retention and Disposal of Information

NECTA retains personal information only for as long as it is required to meet regulatory and operational requirements.

When personal information is no longer required, NECTA takes reasonable steps to securely destroy or de-identify the information to ensure that it cannot be accessed or used inappropriately.

Record Type	Minimum Retention Period
Student enrolment and academic records	30 years from date of last entry
AQF certification documentation	30 years
Financial records	7 years (in accordance with tax and corporate law)
Complaints and appeals records	7 years
Staff employment records	7 years from cessation of employment
PRISMS and ESOS records	As required by DHA and ESOS Act
USI records	As required by the Student Identifiers Act 2014

Data Breach Management

In the event of a data breach, NECTA will take immediate steps to assess the nature and extent of the breach and to contain any risks associated with it. Where required, affected individuals will be notified, and the breach will be reported to the Office of the Australian Information Commissioner (OAIC) in accordance with the Notifiable Data Breaches scheme. NECTA will also review the incident and implement corrective actions to prevent similar breaches in the future.

Data Breach Response Steps

- Immediately report any suspected breach to the Director Academic & Compliance and CEO
- Assess the nature, scope and likely consequences of the breach
- Contain the breach and prevent further unauthorised access or disclosure
- Determine whether the breach is an eligible data breach under the NDB Scheme
- Notify affected individuals as soon as practicable where required
- Report to the OAIC within 30 days if an eligible data breach is identified
- Document the breach, investigation findings and corrective actions
- Implement corrective actions to prevent recurrence
- Record the incident in the Continuous Improvement Register

Access to Personal Information

Individuals have the right to access their personal information held by NECTA and to request corrections if the information is inaccurate, incomplete or outdated. Requests for access or correction must be made in writing. NECTA will respond to such requests within a reasonable timeframe and may require verification of identity before providing access.

Step	Action
1	Individual submits a written request for access or correction to the Administration and Student Support Officer
2	Identity of the individual is verified before access is provided
3	Request is reviewed to confirm it is valid and within scope
4	Access is provided or correction is made within a reasonable timeframe (maximum 30 days)
5	All requests and outcomes are recorded to ensure transparency and compliance
6	Where access is denied, the reason is provided in writing with information on how to escalate

Complaints

NECTA provides a clear process for managing privacy-related complaints through its Complaints and Appeals Policy and Procedures. All complaints are taken seriously and will be investigated in a fair and transparent manner. Individuals will be informed of the outcome of the complaint and may escalate the matter to external bodies if they are not satisfied with the outcome.

- Privacy complaints may be lodged verbally or in writing with the Director Student Experience
- All complaints are acknowledged within 2 business days and investigated promptly
- Outcomes are communicated to the complainant in writing
- Unresolved complaints may be escalated to the OAIC at www.oaic.gov.au
- Refer to NECTA-POL-CMP-001 (Complaints & Appeals Policy) for the full complaints procedure

Website and Cookies

NECTA's website may use cookies and similar technologies to enhance user experience and analyse website traffic. Users have the option to manage or disable cookies through their browser settings. NECTA may also use third-party analytics tools, such as Google Analytics, to collect anonymised information about website usage. NECTA is not responsible for the privacy practices of third-party websites.

Procedures

1. Manage Personal Information

Step	Action
1.1	Process all personal information according to the relevant procedures.
1.2	All information is collected, used, stored and disclosed only for authorised purposes related to training, assessment, student support and compliance obligations.
1.3	Archive personal information according to the relevant procedures.

2. Provide Access to Records

Step	Action
2.1	Review written requests for access to records.
2.2	Review each request to ensure it is valid and that the identity of the individual requesting access is verified.
2.3	Arrange for the individual to access their personal information within a reasonable timeframe, ensuring that access is provided in a secure and appropriate manner.
2.4	Where individuals request corrections to their personal information, NECTA will review the request and update the records where the information is found to be inaccurate, incomplete or outdated.
2.5	NECTA will maintain records of all access and correction requests, including the outcome of each request, to ensure transparency and compliance with privacy obligations.

Responsibilities

Role	Responsibility
Principal Executive Officer (PEO) / CEO	Approves this policy; has ultimate responsibility for privacy governance; authorises any data breach notifications to OAIC.
Director Academic & Compliance	Oversees privacy compliance across all operations; reviews this policy annually; manages data breach response; maintains the Continuous Improvement Register in relation to privacy incidents.
Academic Manager	Responsible for overseeing the implementation of this policy and ensuring that privacy requirements are maintained across all areas of operations.
Administration and Student Support Officer	Responsible for processing all personal information and providing access to records as required; maintains access and correction request records.
IT & Systems Officer	Maintains system security, role-based access controls and backup integrity; manages technical aspects of data breach containment.
All Staff	Must handle all personal information in accordance with this policy and the Australian Privacy Principles; must report any suspected breach or privacy concern immediately.

Approvals and Document Control

This set of policies and procedures has been purchased under a licence agreement with RTO Works and has been reviewed and customised to suit NECTA's specific requirements.

Field	Detail
Document Code	NECTA-GOV-PRV-001
Version Number	V4.0
Status	Approved
Approved By	PEO
Approval Date	14 April 2026
Review Date	On or before 14 April 2027
Regulatory Alignment	Privacy Act 1988 | Australian Privacy Principles | NDB Scheme | ESOS Act 2000 | National Code 2018 Standard 3 | Standards for RTOs 2015 Standard 4.3 | National VET Data Policy | Student Identifiers Act 2014
Related Documents	NECTA-POL-CMP-001 Complaints & Appeals Policy | NECTA-SOP-IT-001 IT & Systems Maintenance SOP | NECTA-SOP-CI-001 Continuous Improvement SOP | NECTA-GOV-POL-001 Policy Framework