

PRIVACY POLICY



Policy Field	Compliance
Document Code	COM-POL-01
Version	V1.0
Date	October 2026
Review Date	October 2027
Responsible Officer	CEO
Standards Referenced	SRTO 2025 Outcome Standard 4.3 SRTO 2025 Compliance Standards ss 10, 12, 16, 20
Other Legislation	Privacy Act 1988 (Cth) and the Australian Privacy Principles, NVR Act 2011, National VET Data Policy and Data Provision Requirements 2020, Student Identifiers Act 2014 (Cth)
Issued by	The CEO



1. Purpose

National Institute of Vocational Studies Pty Ltd, trading as Building Institute NSW, is committed to protecting the privacy and confidentiality of personal information. This policy explains:

- what personal information Building Institute NSW collects, when and why
- how that information is used, stored, protected and disclosed
- how student information is reported to the National Centre for Vocational Education Research (NCVER) and government, in line with the NCVER Privacy Notice
- how people can access or correct their information or make a privacy complaint
- how Building Institute NSW responds to a data breach.

2. Scope

This policy applies to personal information about:

- prospective, current and former students
- parents, guardians or emergency contacts of students
- employers, workplace supervisors and industry contacts
- Advisory Committee members
- Building Institute NSW staff and contractors (to the extent not covered by the employee records exemption in the Privacy Act)
- other stakeholders whose personal information Building Institute NSW collects or holds.

It covers personal information in any form, including paper records, electronic records, emails, recordings, photographs, and information held in the Student Management System (SMS), the Learning Management System (LMS) and cloud services. All governing persons, staff, contractors, Advisory Committee members, external service providers and any person or organisation who is engaged with Building Institute NSW must comply with this policy.

3. Definitions

Term	Meaning
Australian Privacy Principles (APPs)	The 13 principles in Schedule 1 of the Privacy Act that govern how personal information is collected, used, disclosed, stored and corrected.

PRIVACY POLICY



Term	Meaning
AVETMISS	The Australian Vocational Education and Training Management Information Statistical Standard, which sets out the data that RTOs collect and report to NCVER.
De-identified information	Information from which identifiers have been removed so that no individual is reasonably identifiable.
Eligible data breach	Unauthorised access to, disclosure of, or loss of personal information that is likely to result in serious harm to any of the individuals involved, where the harm has not been prevented by remedial action.
National VET Data Collection	The national collection of VET student and training activity data, kept by NCVER, to which RTOs must report under the National Vocational Education and Training Regulator Act 2011 (Cth).
National VET Data Policy	The national policy that sets out how VET data is collected, used and disclosed, including the requirement to give students the NCVER Privacy Notice and Student Declaration at enrolment.
NCVER	The National Centre for Vocational Education Research Ltd, which manages the National VET Data Collection and is responsible for collecting, managing, analysing and communicating research and statistics about the Australian VET sector.
NCVER Privacy Notice and Student Declaration	The standard notice and declaration that RTOs must give students at enrolment, explaining how their personal information is collected, used and disclosed by the RTO, NCVER, the Australian Government department responsible for VET and state or territory training authorities.
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in material form or not.
Sensitive information	A type of personal information that includes racial or ethnic origin, political opinions, religious beliefs, sexual orientation, membership of a professional or trade association or trade union, criminal record, and health, genetic or biometric information.



Term	Meaning
Unique Student Identifier (USI)	A reference number issued under the Student Identifiers Act 2014 (Cth) that every student undertaking nationally recognised training in Australia must have. It links a student's training records across providers and gives access to an authenticated VET transcript.

4. Legislative and Regulatory Framework

Building Institute NSW complies with:

Law or requirement	What it requires
Privacy Act 1988 (Cth), as amended by the Privacy and Other Legislation Amendment Act 2024 (Cth)	Compliance with the 13 APPs and the Notifiable Data Breaches (NDB) scheme.
National Vocational Education and Training Regulator Act 2011 (Cth)	Requires Building Institute NSW to disclose student personal information to the National VET Data Collection kept by NCVER, and authorises disclosure to the relevant state or territory training authority.
National VET Data Policy and the Data Provision Requirements 2020	Require Building Institute NSW to collect AVETMISS data, include the NCVER Privacy Notice and Student Declaration in enrolment, and report data to NCVER.
Student Identifiers Act 2014 (Cth)	Governs how Building Institute NSW collects, verifies, uses and protects USIs.
Standards for RTOs 2025 (Compliance Standards ss 10, 12, 16 and 20; Outcome Standard 4.3)	Records retention, USI verification, notification of significant events, compliance with privacy laws and risk management.

5. How Building Institute NSW Manages Personal Information

Building Institute NSW applies the APPs to all personal information it handles

5.1 Open and transparent management (APP 1)

Building Institute NSW manages personal information openly and transparently. This policy is free, is published on the website, is provided before enrolment and is available on



request, in an alternative format if needed. Building Institute NSW has practices and systems in place to comply with the APPs, including:

- a privacy check before introducing a new system or changing how personal information is handled
- privacy and confidentiality clauses in contracts and agreements with all staff, contractors, external service providers and any person or organisation who is engaged with Building Institute NSW
- regular reviews of this policy and levels of access to each system.

5.2 Anonymity and pseudonymity (APP 2)

People may deal with Building Institute NSW anonymously or using a pseudonym for general enquiries, feedback and some complaints. This is not possible for enrolment, as Building Institute NSW is required by law to identify students, verify their USI and report their training to NCVER, and to provide records to the National VET Regulator or another government agency on request.

5.3 Collection of personal information (APPs 3, 4 and 5)

Building Institute NSW collects personal information only where it is reasonably necessary for its functions as an RTO or required by law, and only by lawful and fair means. The information collected may include:

Category	Examples
Identity and contact	Name, date of birth, gender, address, phone, email, emergency contact, photo identification, citizenship or residency status
Additional National VET data (AVETMISS)	USI, highest school level completed, prior educational achievement, labour force status, country of birth, language spoken at home, English proficiency, Aboriginal and Torres Strait Islander status, disability status and reason for study
Suitability and support	LLND assessment results, résumé, qualifications and Statements of Attainment, work history, goals, intended licensing outcomes, and any disability, health or other support needs
RPL evidence	The RPL application, portfolio of evidence, interview notes and suitability review outcome
Training records	Enrolment details, Confirmation of Enrolment, assessment evidence and results, RPL and credit transfer records, and certificates issued



Category	Examples
Financial	Payment and billing information and refund records
Communications	Emails, texts, notes of conversations, complaints, appeals and feedback
Digital	LMS login and activity records, and recordings of online sessions where students are told in advance

When information is collected

Personal information is collected at the points shown in the pre-enrolment and enrolment flowcharts:

Stage	Information collected
Enquiry	Contact details, goals and course interest, recorded with the name of the staff member who received the enquiry
Pre-enrolment including suitability reviews	Application to Enrol Form, USI, photo identification, eligibility and supporting documents, LLND results (if applicable), resume (if applicable) AQF Certification for credit Transfer Application Form (if applicable), the RPL application and portfolio of evidence (if applicable), work history, previous study
Enrolment and induction	Signed agreements and payment details

Collection notices

At or before the time of collection, Building Institute NSW tells people:

- who Building Institute NSW is and available contact methods and time
- why the information is being collected, and whether the law requires it
- how it will be used and who it may be disclosed to, including NCVER, the National VET Regulator and state or territory training authorities if applicable
- what happens if they do not provide it (for example, a person cannot be enrolled without the information the law requires)
- whether it is likely to be disclosed overseas
- how to access or correct it and how to make a complaint.



5.4 Sensitive information

Sensitive information is collected only with the person's consent and only where it is reasonably necessary. Telling Building Institute NSW about a disability or health condition is always voluntary. Some sensitive information, such as Aboriginal and Torres Strait Islander status and disability status, is collected because it is required for national VET data reporting. Sensitive information is used only for the purpose it was given, such as planning reasonable adjustments or reporting national VET data, and access to it is restricted.

5.5 Unique Student Identifier (USI)

- Each student's USI is collected at application and verified with the Student Identifiers Registrar before it is used, as required by section 12 of the Compliance Standards.
- The USI is included in data reported to NCVER, so the student's results appear in their authenticated VET transcript.
- The USI is never printed on a certificate or Statement of Attainment, and USI information is handled only as authorised by the Student Identifiers Act 2014 (Cth).

5.6 Use and disclosure (APP 6)

Building Institute NSW uses personal information to deliver VET courses and, as needed, to meet its obligations as an RTO, including to:

- process and manage enrolments, and assess suitability and support needs
- deliver training and assessment, and provide support and reasonable adjustments
- issue certificates and keep records
- manage fees, payments and refunds
- handle complaints and appeals
- report to NCVER, regulators and funding bodies
- carry out quality assurance, validation and continuous improvement.

Personal information is used and disclosed only for the purpose it was collected for, or for a related purpose the person would reasonably expect, unless the person consents or the law requires or authorises it. Building Institute NSW may disclose personal information to:

Recipient	Purpose
NCVER (National VET Data Collection)	Required by the NVETR Act.
State or territory training authority	Authorised by the NVETR Act, and required where the student is in a government-funded program.
National VET Regulator	Regulatory monitoring, audits and investigations.



Recipient	Purpose
Student Identifiers Registrar	Verifying or creating USIs.
Australian Government departments and funding bodies	Administering funding programs, apprenticeships and traineeships, and incentives.
Australian Apprenticeships Support Network providers	Where the student is an apprentice or trainee.
Employers	Where the employer is paying for or supporting the training (including apprentices and trainees, whose employer attends the pre-training review), and only with the student's consent.
External service providers	External service providers, LMS and cloud providers that need the information to provide services to Building Institute NSW and are bound by confidentiality.
Others	With the person's consent, or where the law requires or authorises it, for example to lessen a serious threat to someone's life, health or safety, or in response to a court order.

Building Institute NSW does not sell, rent or trade personal information.

5.7 Direct marketing (APP 7)

Building Institute NSW uses personal information to respond to enquiries and provide requested course or service information where a person would reasonably expect it or has consented. Enquiry details are not used for ongoing promotional messages or given to anyone else for marketing. Sensitive information, and information obtained through NCVER or government reporting, is never used for marketing.

5.8 Cross-border disclosure (APP 8)

Building Institute NSW assesses privacy and security risks associated with cloud-based systems and overseas service providers before sharing personal information. Where an arrangement involves cross-border disclosure, Building Institute NSW will document an assessment under APP 8 and take reasonable steps to ensure appropriate protection of the information, including contractual safeguards and oversight. Relevant privacy notices, including this policy and the Application to Enrol Form, will be updated, and affected students informed before any material change takes effect.



5.9 Government-related identifiers (APP 9)

Building Institute NSW assigns its own Student ID through its SMS and does not use government identifiers, such as a USI, Medicare number or tax file number, as its internal Student ID. Government identifiers are used or disclosed only as the law permits.

5.10 Quality of personal information (APP 10)

Building Institute NSW takes reasonable steps to make sure the personal information it collects, uses and discloses is accurate, up to date, complete and relevant. Students are asked to update their details within 7 days of any change, and AVETMISS data is checked using NCVER's validation software before it is reported.

5.11 Security of personal information (APP 11)

Building Institute NSW takes reasonable steps, including technical and organisational measures, to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. These include:

- role-based access, so each person can only see the information they need for their role, with access removed promptly when someone leaves
- Password and multi-factor authentication on systems holding personal information
- encryption of data in transit and, where available, at rest
- secure, locked storage for any paper records
- regular software updates, backups and security monitoring
- secure methods for sending personal information
- privacy and cyber security training for all staff at induction and each year, including how to recognise phishing and report a suspected breach
- contractual privacy and security obligations for any service providers and checks of their security arrangements.

5.12 Retention and destruction

Records are kept for as long as the law and Building Institute NSW's regulatory obligations require, including:

Record	Minimum retention
AQF certification documentation issued (qualifications and statements of attainment) and the certification register	30 years from issue



Record	Minimum retention
Completed student assessments, including partly completed assessments on withdrawal and RPL evidence	2 years after the student completes the training product
Complaints and appeals records	7 years from closure of complaint of appeal
Financial records, including fee and refund records	7 years after the transactions they cover
Tax records	5 years from lodgement, kept with financial records for 7 years
Employee records	7 years after the record is made
Records of notifiable WHS incidents	At least 5 years from the notification of the incident
Validation records and assessment tool reviews	At least 5 years
Training and Assessment Strategies, marketing material and pre-disclosure information	At least two years after the TAS is superseded or the final student studying under that TAS completes the relevant training product, whichever is later.
Governance records and registers, such as minutes, independent adviser engagements and conflict checks; written delegations and appointment authorities; investigative findings; notifications to the National VET Regulator.	7 years

When personal information is no longer needed for any lawful purpose, it is securely destroyed or de-identified (for example, by secure shredding or permanent deletion), in line with the Records Management Policy. If Building Institute NSW stops operating, student certification records are transferred to the National VET Regulator as required.

5.13 Access and correction (APPs 12 and 13)

- People can ask to see the personal information Building Institute NSW holds about them. Their identity is verified before access is given.
- Building Institute NSW responds within 30 days. There is no charge to make a request, although a reasonable charge may apply for copies of large volumes of records. Any charge is advised in advance.



- If information is inaccurate, out of date or incomplete, it is corrected. Corrected AVETMISS data is resubmitted to NCVER.
- If access or correction is refused, the person receives written reasons and is told how to complain. A person whose correction request is refused can ask for a statement to be attached to the record.
- Under the NCVER Privacy Notice, students wanting to access or correct information held by NCVER should contact Building Institute NSW first.

5.14 Automated decision-making

Building Institute NSW does not use computer programs, automated systems or artificial intelligence that use personal information to make, or substantially help make, decisions that could significantly affect a person's rights or interests, such as enrolment, assessment or refund decisions.

5.15 Serious invasions of privacy

Building Institute NSW's practices are designed to make sure no student, staff member or stakeholder experiences a serious invasion of privacy through its actions.

6. National VET Data and the NCVER Privacy Notice

Building Institute NSW must ensure students who provide personal information that is included in the National VET Provider Collection are aware of how the information may be collected, used or disclosed and provide the required Privacy Notice as published under the current National VET Provider Collection Data Requirements Policy. Building Institute NSW provides the required Privacy Notice in its Application to Enrol Form. The published version and effective date must be regularly checked when the form is reviewed and whenever changes to the Privacy notice are announced. Any updates must be incorporated before the revised requirements take effect. Applicants must read the notice and complete an acknowledgment on the Application to Enrolment form before enrolment.

7. Privacy Complaints

Information about how to lodge a complaint is provided in the Complaints Policy, which is published on Building Institute NSW's [website](#), included in the pre-disclosure information provided to applicants prior to enrolment and available on request.

8. Data Breach Response Procedure

If Building Institute NSW suspects or becomes aware of a data or cyber security breach involving personal information, it follows the procedure below, in line with the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act and the OAIC's guidance. Examples



include a lost laptop or phone, an email sent to the wrong person, a hacked account, a ransomware attack, or a service provider being compromised.

8.1 Step 1: Contain

- Immediately secure systems and stop any further unauthorised access or disclosure.
- Suspend compromised accounts, reset passwords, revoke access or disable affected systems with the external IT provider.
- Ask anyone who received information in error to delete it and confirm they have done so.
- Retrieve or secure any personal information that has been disclosed, where possible.
- Keep evidence, such as logs and emails, for the assessment.
- Report the incident to the CEO straight away, or to the Director if the CEO is unavailable.

8.2 Step 2: Assess

- The CEO leads the assessment, with support from an external IT provider.
- Identify the type of information involved (for example identity, financial, health or USI information), the number of people affected and the cause.
- Assess whether the breach is likely to result in serious harm to anyone (for example identity theft, financial loss, or emotional or reputational harm), and whether remedial action can prevent that harm.
- Take all reasonable steps to complete the assessment within 30 days.

8.3 Step 3: Notify

If the breach is an eligible data breach, Building Institute NSW will, as soon as practicable:

- notify the OAIC using the Notifiable Data Breach form
- notify affected people directly (or, if that is not practicable, publish a statement), explaining what happened, the information involved and the steps they should take to protect themselves, such as changing passwords or contacting IDCARE (1800 595 160)
- assess whether the breach significantly affects Building Institute NSW's ability to meet its obligations and, if so, notify the National VET Regulator within 10 business days under section 16 of the Compliance Standards
- notify any other government body or organisation as required by contract or law
- report cyber incidents to the Australian Cyber Security Centre through ReportCyber
- inform the Director immediately.



8.4 Step 4: Record

Record the breach in the Risk Management Register and the Continuous Improvement Register, whether or not it is notifiable, including the date and time of the breach and when it was discovered, the systems and information affected, the steps taken to contain, assess and notify, and recommendations for follow-up.

8.5 Step 5: Review and prevent

- Carry out a post-incident review to identify the root cause.
- Implement corrective and preventive actions, including improvements to policies, systems and staff training, to address underlying causes and reduce the likelihood of recurrence.
- Report the outcome to the Director and the Advisory Committee as part of risk management and governance reporting.

9. Roles and Responsibilities

Role	Responsibilities
Director	Receives immediate notice of any data breach and the CEO's quarterly privacy report.
CEO	Accountable for Building Institute NSW's compliance with privacy law, and makes sure privacy risks are managed and resources are available. First point of contact for privacy enquiries, access and correction requests. Leads data breach responses and notifications to the OAIC and affected people. Maintains the Privacy Notice in the Application to Enrol Form
Student Enrolment Officer	Collects and records enrolment information accurately, makes sure every applicant receives the NCVER Privacy Notice and acknowledges the privacy notice in the form, verifies USIs, and supports AVETMISS reporting through accurate record keeping. Helps students with privacy concerns and refers matters to the CEO or director.
Trainers and Assessors	Handle student information in line with this policy, use only approved systems, and report any suspected breach immediately.

11. Monitoring and Review

The CEO monitors compliance with this policy through privacy complaints, incident reports, access requests, system access reviews and internal audits, and reports to the Director and Advisory Committee through quarterly reports and summaries

PRIVACY POLICY



This policy and the Privacy Notice in the Application to Enrol Form are reviewed at least once a year, and sooner if privacy law, the NCVER Privacy Notice, the National VET Data Policy, the Standards for RTOs or Building Institute NSW's systems change.

12. Related Documents

- Application to Enrol Form
- Complaints Policy
- Appeals Policy
- Consumer Protection Policy
- Access and Equity Policy
- Governance and Management of RTO Policy
- Advisory Committee Policy and Procedure
- Student Experience Guide
- Records Management Policy
- Student Recruitment and Pre-Enrolment Policy
- Risk Management Register and Continuous Improvement Register