

RTO	Builders Academy Australia (RTO ID 21583)
Type	Public
Applicable standards	Standards for Registered Training Organisations 2025 State and Territory Funding contracts Higher Education Support Act 2003 Australian Privacy Principles (APP) 2014 The Privacy Act 1988 (Commonwealth) Privacy Amendment (Enhancing Privacy Protection) Act 2012 Student Identifiers Regulation 2014 Identity Verification Services Act 2023 (Cth)
Authorised by	General Manager - Quality, Education and Compliance
Effective Date	29 September 2026
Version	V3.2

Student Privacy Policy

Overview

Builders Academy Australia (BAA) is required to collect, use, store and disclose a range of personal information on students, employees, and a range of other stakeholders. BAA complies with the Privacy Act 1988 (Cth), including the 13 Australian Privacy Principles (APP) as outlined in the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth). BAA is committed to maintaining the privacy and confidentiality of its RTO personnel, RTO contractors, third party and participant records.

This Policy specifically relates to the privacy of student, employer and other groups or individuals in the relation of training and / or assessment services. As such, this Policy applies to all staff, contractors and other third parties which may be privy to sensitive information covered by the APP.

Alignment with Standards for RTOs 2025

This policy supports compliance with the Standards for RTOs 2025, particularly the following clauses from the Compliance Standards:

- **Clause 3.1:** Ensuring student records are securely maintained and accessible to support enrolment, training, and assessment outcomes.
- **Clause 7.1:** Ensuring students are aware of their privacy rights and enabling complaints and feedback mechanisms regarding the handling of personal data.
- **Clause 8.2:** Maintaining evidence of compliance through secure and retrievable recordkeeping practices.

This policy is reviewed annually and updated in response to legislative or operational changes and feedback from staff, students, and external stakeholders.

What is the APP?

In 2014, the APP replaced the National Privacy Principles (NPP). The APP broadly covers a range of private information that BAA may obtain in the course of our normal duties. For our purposes, these include, but are not limited to:

Student

1. Student identifiers (name, date of birth, student numbers, unique student identifiers (USI), State and Territory Student Identifiers and Apprenticeship / Traineeship Contract IDs.
2. Student contact details (phone, address, email, fax etc.).
3. Information such as disabilities, illness, language, literacy or numeracy challenges, and other sensitive information.
4. Student IDs such as Medicare cards, driver's license, concession cards etc. for the purpose of identifying eligibility for courses and / or funding.
5. Student residency and or citizenship status for the purpose of identifying eligibility for courses and or funding.
6. Copies of student transcripts from other education institutes for determining eligibility for course and / or credit transfers.
7. Third party reports regarding on-the-job performance for employers; and
8. Assessment results

Employer/Third Parties

1. Commercially sensitive information about employers and other third parties; and
2. Employer/Third Parties contact details (Phone, address, email, fax, etc.)

Through this policy BAA seeks to ensure that you will be able to deal with the Registered Training Organisation (RTO) with confidence that personal information is only used by the organisation in the ways that are legal, ethical, and secure.

BAA will only collect personal information from individuals by fair and lawful means which is necessary for the functions of BAA. BAA will only collect sensitive information with the consent of the individual and if that information is reasonably necessary for the functions of BAA. By entering into an enrolment contract, individuals provide informed consent for Builders Academy Australia (BAA) to collect, store, and disclose personal information as outlined in this policy.

Where BAA collects personal information from third parties—such as employers, job services providers, or via a third-party identity verification system—students will be informed at the time of enrolment or via direct communication.

For use of images, video, or personal details on public platforms (including social media), BAA will obtain **express written consent** outlining the potential for international access and advising students of the associated risks.

The information requested from individuals by BAA will only be used to provide details of study opportunities, to enable efficient course administration, to maintain proper academic records, to assess an individual's entitlement to state or territory government funded courses, to apply for with permission or check a Unique Student Identifier and to report to government agencies as required by law. If an individual chooses not to give BAA certain information, then BAA may be unable to enrol that person in a course or supply them with appropriate information.

Who we Disclose Student Information to:

Broadly speaking, we will only disclose information to the following persons:

- To you, the student.
- To relevant State / Territory and Federal education and funding Government bodies. By entering into an enrolment contract, Students consent for this information to be disclosed.

- To your employer if you are an apprentice or trainee, or your employer is paying for the cost of your course directly to BAA.
- To a third party who is paying for your course (as nominated on the Authority to Invoice form).
- To your legal guardian or parent if you are under 18.
- To other persons as directed by you.
- To other persons where you have provided verbal or written consent for us to do so.
- Where directed by law to release information.

Government Bodies

Personal information about students studying with BAA may be shared with the Australian Government, State and Territory Governments and designated authorities, including the Australian Skills Quality Authority (ASQA). This information includes personal and contact details, course and unit enrolment details and changes.

BAA will not disclose an individual's personal information to another person or organisation unless:

- a) the individual concerned is reasonably likely to have been aware or made aware that information of that kind is usually passed to that person or organisation
- b) the individual concerned has given written consent to the disclosure.
- c) BAA believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person.
- d) the disclosure is required or authorised by or under law OR
- e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

Where personal information is disclosed for the purposes of enforcement of criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of public revenue, BAA shall include in the record containing that information a note of the disclosure. Any person or organisation that collects information on behalf of BAA or to whom personal information is disclosed as described in this procedure will be required not to use or disclose the information for a purpose other than the purpose for which the information was collected by them or supplied to them.

Identity Verification Services

As part of BAA's enrolment and eligibility processes, we may need to verify identity information provided by students. Identity verification may be required to meet applicable enrolment, government funding, regulatory or other legal requirements.

BAA may use a third-party identity verification system to verify information contained in an identity document against records held by the relevant document issuer or official record holder. Before identity information is submitted for verification, BAA will provide the individual with information about the verification process and obtain their express consent. Individuals who do not consent to verification through the third-party system will be advised of available alternative methods of identity verification.

Personal information collected for identity verification is handled in accordance with this Policy, the Privacy Act 1988 (Cth), the Australian Privacy Principles and other applicable requirements.

1. Information Used for Identity Verification

BAA may collect identity information necessary to verify an individual's identity and to meet applicable enrolment, government funding, regulatory or legal requirements. This may include

information contained in government-issued identity documents such as a driver's licence, Medicare card, passport or birth certificate.

BAA will only collect and use identity information that is reasonably necessary for the applicable verification purpose.

2. Consent to Identity Verification

Before information is submitted through a third-party identity verification system, the individual will be provided with information about the verification process and asked to provide express consent. Identity information will not be submitted for verification unless the required consent has been obtained.

3. Handling and Retention of Identity Information

BAA takes reasonable steps to protect identity information from misuse, interference, loss, unauthorised access, modification or disclosure.

Identity information collected for the purpose of performing an identity verification request is not retained by BAA after it has been used for that purpose. BAA may retain information necessary to evidence that the required identity verification has been completed and to meet applicable recordkeeping, audit, regulatory or contractual requirements.

Where personal information from an identity document is retained as part of a student record for an authorised purpose, BAA does not retain the identity document number unless retention is otherwise required or authorised by law.

4. Alternative Methods of Identity Verification

Individuals are not required to use BAA's third-party identity verification system where an alternative method of identity verification is available.

Where an individual does not consent to verification through the third-party system, BAA will advise them of an appropriate alternative method of verifying their identity. This may include sighting acceptable identity evidence or another reasonable and secure verification method that satisfies the applicable enrolment, regulatory or funding requirements.

5. Questions, Rights and Complaints

Individuals may contact BAA if they have questions about the collection, use, disclosure or handling of their personal information for identity verification, wish to request access to or correction of their personal information, or wish to make a privacy complaint.

Requests and complaints will be managed in accordance with this Policy and BAA's applicable complaints and privacy processes.

The Following Outlines How We Apply Each Privacy Principle:

APP 1	Open and Transparent Management of Personal Information	➤ We publish this policy on our website: www.buildersacademy.com.au. ➤ A link to this policy is included in our student handbooks. ➤ BAA outlines what information is collected and what it will be used for, what information will be released and under what conditions.
-------	---	--

APP 2	Anonymity and Pseudonymity	➤ Individuals can remain anonymous for the purpose of requesting general information on a course, website enquiries or anonymous complaints/feedback. ➤ Individuals who wish to undertake nationally recognised training with BAA will be required to disclose information of a personal nature as outlined in this policy. ➤ Students who wish to provide feedback on our courses or services may do so anonymously.
APP 3	Collection of Solicited Personal Information	➤ BAA will collect information you provide on enrolment in a nationally accredited course or on commencement of employment with BAA. We may also collect information you provide on websites, enrolment forms, course materials and assessments. ➤ BAA may sometimes collect information, with your consent, from your employer, a job services provider, or other organisations where students may engage in placement for training and assessment purposes. ➤ BAA collects information of a personal and sometimes sensitive nature. Information BAA collects may include: full name, date of birth, residential address, contact details, demographic information, ability/disability, employment details, educational background, indigenous background, concession status language, literacy and numeracy skills and educational/course progress. BAA may also collect information on your next of kin or parent/guardian for emergency purposes.
APP 4	Dealing with Unsolicited Personal Information	➤ BAA only collects uses and stores information which is directly related to the provision of training and assessment (for students) and information directly related to the employment or engagement of contractors (for employees and contractors). ➤ Information which is received that is not related to training and assessment or employment with BAA is destroyed in a safe and secure manner.
APP 5	Notification of The Collection of Personal Information	➤ Students and employees are notified when information is collected or sourced from third parties. Such notifications are expressed in enrolment forms, assessment tools and other written documents or implied in such circumstances such as workplace observations.
APP 6	Use or Disclosure of Personal Information	➤ BAA only uses information for the provision of training and assessment BAA only discloses information to 3rd parties such as: i. Relevant Government bodies ii. Apprenticeship Centres – where a student is a trainee or apprentice iii. Employers – where a student is a trainee or apprentice or when an employer has paid for the provision of training

		iv. Job Services Providers – where you have been referred by a Job Service Provider v. External auditors and our consultants vi. Parent/Guardian – where a student is under the age of 18 vii. Other entities required by law
APP 7	Direct Marketing	➤ Your personal information will never be sold to any marketing company or third party. ➤ BAA may use your personal information to market directly to you only for the provision of further training and assessment with the RTO. ➤ BAA will only use your information if you have provided consent to use your information for this purpose and you have opted in to this type of communication. ➤ BAA will provide an 'opt out' option for receiving direct marketing.
App 8	Cross-Border Disclosure of Personal Information	➤ BAA will not disclose your personal information to any entity outside of Australia unless you have provided your express written consent. ➤ All records will be kept in Australia. ➤ Students who agree to BAA to using their personal information such as name and images for marketing purposes via social media platforms, are advised of the possibility of their information being accessed by individuals overseas.
APP 9	Adoption, Use or Disclosure of Government Related Identifiers	➤ BAA is required to collect, in some circumstances, government related identifiers. BAA will not use these identifiers for any reason or purpose except for the explicit reason it is required (e.g., Concession numbers, USI, Driver's License Number, etc.) and will not use these numbers as an identifier of individuals. ➤ BAA will only disclose government related identifiers where required by law or express consent has been given to disclose this information.
APP 10	Quality of Personal Information	➤ BAA collects information and ensures it is accurate, up to date and complete. ➤ BAA will take all reasonable steps to ensure that the information provided by individuals is correct and any third-party information received can be verified for accuracy, currency, and completeness.
APP 11	Security of Personal Information	➤ All personal and sensitive information is kept safe and secure at all times; only authorised BAA staff may access this information. ➤ Destruction of personal and sensitive information is carried out by commercial document destruction companies or secure shredding or secure electronic deletion.
APP 12	Access to Personal Information	➤ Individuals may request copies of information which is kept about them at any time.

		➤ BAA will not release personal information to a third party unless they are authorised to do so. ➤ When requesting personal information, the individual will need to be able to adequately identify themselves. ➤ The timeframe for granting access will vary according to the nature of the request, the person who is requesting the information and how the information is requested to be given. For example, information requested by a phone call will generally be given during the call if the caller's identity can clearly be established and the requestor is wanting information verbally. More complex requests may take longer. Please allow 5-10 working days. Where we are unable to respond to a request within this time frame, we will advise you.
APP 13	Correction of Personal Information	➤ Individuals who feel that the information BAA uses, and stores is inaccurate, or incomplete may request to have the information updated and corrected. Such corrections must be in writing to: enquiries@buildersacademy.com.au mailto:privacy@buildersacademy.com.au

Responsible Parties and Review Information

Privacy Compliance Training

Staff who handle personal information or use identity verification systems must undertake training on student privacy:

1. Upon commencement of employment.
2. At least every two years thereafter.
3. **Immediately** when there are:
 - Significant changes to the **Privacy Act**, **APPs**, or **identity verification requirements**
 - Changes to **internal systems** used for identity verification
 - A privacy breach involving identity information
4. When directed.

As BAA is a member of UP Education, the HR department may direct all staff within the group to undertake general privacy training. This is at the discretion of the HR department.

The following table outlines the broad kinds of privacy training that are undertaken by BAA staff:

Training Type	Topics Covered	Delivery Method
Induction / Refresher Privacy Training directed by HR Department	An overview of: • Australian Privacy Principles (APP) • Australian Privacy Act 1988	Online via UP Education Personal Learner Management System May also be delivered face-to-face by: • HR Staff • Legal Staff • External privacy experts
Dedicated Privacy Training specific to BAA	Privacy training will generally cover the following topics: • Australian Privacy Principles (APP) • Australian Privacy Act 1988 – Overview • How privacy standards apply to RTOs and individual roles • Relevant BAA forms, privacy declarations and consent forms	This training is role specific and will vary according to the needs of the role the staff member is undertaking. This training may be delivered by a live online webinar accessed through live webinar technology, a recorded webinar accessed through the BAA Learner Management System, or face-to-face. Live sessions may be delivered by: • A member of the Compliance Team • The staff member's Team Leader or Manager
Identity Verification Privacy	Comprehensive training on the legal basis for identity verification,	Delivered during staff onboarding and repeated at least every 2 years

Training	operational use of approved identity verification systems, obtaining and documenting informed consent, procedures for handling and verifying identity information, secure handling of personal information, privacy and security incident response protocols, and applicable legislative, regulatory and contractual obligations.	via LMS modules or live compliance-led sessions; ad hoc training provided after legislative changes or identified breaches Initial on-boarding and refresher every 2 years via LMS or live sessions by Compliance or HR
Embedded within other professional development training	Professional development topics which may involve specific processes and procedures that relate to privacy concerns. Examples of these may include, but are not limited to: • Complaints handling and recording training • Training / information sessions on Standards for Registered Training Organisations relating to student and employer data • Training on funding contracts • Training on enrolment processes • Training on archiving processes • Training on databases which contain student and / or employer data	This training is role specific and will vary according to the needs of the role the staff member is undertaking. This training may be delivered by a live online webinar accessed through live webinar technology, a recorded webinar accessed through the BAA Learner Management System, or face-to-face. Live sessions may be delivered by: • A member of the Compliance Team • The staff member's Team Leader or Manager • Another Team Leader, Manager or Senior Staff member as applicable to the topic being delivered.

Additional Privacy Training

Additional privacy training will be delivered to relevant staff when any of the following occur:

- Amendments to the Privacy Act 1988 (Cth) or the Australian Privacy Principles (APPs);
- Changes to privacy obligations under federal legislation, state/territory funding contracts, or the Identity Verification Services Act 2023 (Cth);
- Implementation of new or revised internal procedures, systems, or forms related to the collection, disclosure, or management of personal information;
- As part of continuous improvement initiatives that affect privacy governance or student/employer data handling;
- Following the identification of a privacy breach or high-risk event requiring targeted mitigation strategies.

Privacy Breach Notification Procedure

In the event of a suspected or actual privacy breach, BAA will take the following steps:

1. **Contain** the breach and secure the information;
 2. **Assess** the nature and extent of the breach within 48 hours;
 3. **Notify** affected individuals and the Office of the Australian Information Commissioner (OAIC) within 72 hours if the breach is likely to result in serious harm;
 4. **Review** internal systems to prevent future occurrences.
- All privacy breaches are documented and reviewed through the Continuous Improvement Register.

Additional notification requirements for identity verification incidents

Where a suspected or actual privacy or security breach relates to BAA's use of an identity verification service, the matter must be immediately escalated to the Compliance Team.

The Compliance Team will assess the incident against any additional notification requirements applicable to BAA's identity verification arrangements and coordinate any required external notification within the applicable timeframe.

Applicable external governance, reporting and notification requirements are set out in BAA's **Governance Framework and relevant supporting policies and procedures**.

Personnel must not make external notifications on behalf of BAA unless authorised to do so.

Feedback, Complaints and Appeals

If you wish to lodge a complaint about how BAA handles personal information or if you feel that BAA has breached the Privacy Act, we encourage you to let us know as early as possible.

BAA has a Grievance, Complaints and Appeals Policy that outlines how to provide informal feedback or lodge a formal complaint or appeal. This policy is available on our website. You may choose to remain anonymous.

We treat all feedback with respect and confidentiality, and we aim to resolve issues promptly, fairly, and in a culturally safe manner, accessible to all students and protects students who raise issues. Students may also contact Student Services or their Student Success Coach for assistance in accessing the process.

Our Grievance, Complaints and Appeals Policy is located on the following webpage:

<https://buildersacademy.edu.au/baa-academy-links-and-documents/>

Monitoring and Review

This policy is maintained under version control to ensure it remains accurate, relevant, and compliant with all applicable requirements.

It will be formally reviewed on an annual basis by the Compliance Team, in consultation with relevant stakeholders, including Student Support, Training Operations, and Senior Management.

Reviews will ensure that the policy continues to meet the requirements of the Standards for RTOs 2025, Government contracts, and other regulatory or quality frameworks.

In addition to scheduled reviews, this document may be updated earlier in response to:

- Changes in legislation, regulatory standards, or contractual obligations;
- Internal audits or findings from complaints, appeals, or investigations;

- Feedback from students, staff, or third parties that identifies a need for improvement;
- Organisational restructuring or operational changes that affect policy content.

Where relevant, students and stakeholders will be notified of significant changes via internal communications, staff briefings, or updates to the Student Handbook or website.

Accessibility of Information

BAA is committed to providing support information in accessible formats for students (e.g., plain English, large print, accessible PDFs, translated materials, and formats for assistive technology users).

If required, please speak with your Student Success Coach or Student Services team so we can offer the right support in getting information in an accessible format for you.

We acknowledge the Traditional Custodians of the lands we live on. We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

Appendix – Australian Privacy Principles (APP) Compliance Summary Table

APP No.	Privacy Principle	BAA Compliance Summary
APP 1	Open and Transparent Management	Privacy Policy is published online and linked in student handbooks.
APP 2	Anonymity and Pseudonymity	Anonymous feedback and general enquiries are accepted; identity required for enrolment.
APP 3	Collection of Solicited Personal Information	Collected through enrolment forms, assessments, and authorised third parties with student consent.
APP 4	Dealing with Unsolicited Personal Info	Unsolicited data not required for training/employment is securely destroyed.
APP 5	Notification of Collection	Notification included in enrolment forms, assessments, and verbally where relevant.
APP 6	Use or Disclosure of Personal Information	Disclosed only with consent or legal requirement (e.g. employers, government bodies, parents/guardians).
APP 7	Direct Marketing	Used only for BAA courses; opt-in required; opt-out always available.
APP 8	Cross-Border Disclosure	Express written consent required; marketing examples include social media with international visibility.
APP 9	Adoption of Government Identifiers	Used only for specific legal purposes (e.g. USI, concession checks); not used as personal identifiers.
APP 10	Quality of Personal Information	Regularly validated and updated through student and third-party input.
APP 11	Security of Personal Information	Secured via access controls, physical and digital safeguards, and secure destruction.
APP 12	Access to Personal Information	Requests handled within 10 business days; identity verification required.
APP 13	Correction of Personal Information	Correction requests accepted in writing and actioned within a reasonable timeframe.