Privacy Policy and Procedure

1. Purpose

Australian Learning Group (ALG) is committed to protecting the privacy of personal information collected from students and prospective students.

This Policy and Procedure outlines how ALG collects, uses, stores, secures and discloses student personal information in accordance with:

- *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs)
- *Education Services for Overseas Students Act 2000* (ESOS Act)
- *National Code of Practice for Providers of Education and Training to Overseas Students 2018*
- National VET Data Policy
- *National VET Regulator (Data Provision Requirements) Instrument 2020*

The policy ensures that personal information is handled lawfully, transparently and securely while supporting ALG's obligations as a registered training organisation and CRICOS provider.

2. Definitions

Personal Information: This is information or an opinion about an identified individual, or an individual who is reasonably identifiable.
Examples include:

- name
- address
- date of birth
- contact details
- enrolment records
- academic results
- visa details
- financial information.

Sensitive Information: This is Information relating to an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- criminal record
- health or medical information
- biometric information.

Sensitive information is given a higher level of protection under the Privacy Act 1988.

Disclosure: Disclosure means the release of personal information to another organisation or individual.

Student Management System: The electronic system used by ALG to record, store and manage student information and training records.

3. Scope

This policy applies to:

- prospective students
- current students
- former students
- international students studying under CRICOS courses

This policy applies to the collection, use, disclosure, storage and disposal of student personal information collected by ALG through:

- enrolment forms and applications
- student management systems
- websites and online portals
- student support services
- course administration processes
- government reporting obligations.

This policy does not apply to staff employment records.
ALG websites may contain links to third-party websites. Where students access external sites, the privacy practices of those sites apply and are outside ALG's control.

4. Responsibilities

Admissions Team: Collect student personal information during enrolment and ensure information provided by students is recorded accurately.

Administration Team: Maintain student records, process requests for access or correction of personal information and ensure records are securely stored.

Quality Assurance Team: Ensure personal information is handled in accordance with applicable legislation and regulatory reporting obligations; Coordinate assessment, escalation, reporting and record management activities relating to actual or suspected privacy incidents and data breaches.

IT Team: Maintain secure systems and controls to protect personal information from unauthorised access, misuse or loss.

5. Policy

ALG collects and manages student personal information only where it is reasonably necessary to deliver education services, administer enrolment and meet regulatory obligations.

ALG handles personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

ALG is committed to:

- collecting only information necessary for its operations
- informing students about why their information is collected
- protecting personal information from misuse, loss or unauthorised access
- taking reasonable steps to ensure personal information is accurate, complete, current and up to date
- allowing students access to their personal information
- only disclosing information where authorised by law or with consent.

Where lawful and practicable, individuals may interact with ALG anonymously or using a pseudonym. However, due to the nature of ALG's education services and regulatory obligations, ALG generally requires individuals to provide verified identity information for enrolment, student administration, certification, visa compliance and regulatory reporting purposes.

5.1 Collection and Use of Personal Information

Personal information collected by ALG may be used for:

- processing applications and enrolments
- delivering training and assessment
- issuing AQF certification
- student support and welfare services
- regulatory reporting
- improving services and educational outcomes
- communicating with students regarding their enrolment and studies
- providing information about ALG services, events, pathway opportunities and related educational offerings where permitted by law.

Individuals may opt out of receiving non-essential marketing or promotional communications by using 'unsubscribe' functions or contacting ALG directly.

ALG complies with all government reporting obligations including requirements to provide student activity data to the National Centre for Vocational Education Research (NCVER), government agencies and regulators where required by law.

The NCVER Privacy Notice is provided to students as part of the Letter of Offer and Student Agreement process prior to enrolment.

Sensitive information will only be collected where:

- the student has given consent
- the information is reasonably required
- the collection is authorised or required by law.

Overseas students are required to inform ALG of their current residential address within 7 days of arriving in Australia and within 7 days of any change to their residential address while in Australia. ALG records and maintains this information to support its ESOS and National Code reporting and monitoring obligations.

Students may be contacted to participate in surveys conducted by NCVER, government departments or authorised third parties. Students may opt out of these surveys at the time they are contacted.

Where ALG receives personal information that was not requested and is not reasonably required for its operations or legal obligations, ALG will take reasonable steps to destroy or permanently de-identify the information as soon as practicable in accordance with the Privacy Act 1988.

5.2 Disclosure of Personal Information

ALG may disclose student personal information where authorised or required by law, including to:

- government departments and regulators
- NCVER
- ASQA
- the Tuition Protection Service (TPS)
- Department of Employment and Workplace Relations (DEWR)
- education agents acting on behalf of the student
- other education providers for credit transfer or pathway purposes
- employers where training is employer-funded
- third-party service providers engaged by ALG to support operations and student services.

Personal information may also be transferred where ALG undergoes a business restructure, merger, acquisition or transfer of business operations, subject to applicable privacy obligations.

ALG does not disclose personal information to other third parties without consent unless disclosure is authorised or required by law.

Student personal information may be stored in or accessed through cloud-based systems or third-party service providers, including providers located overseas. Where overseas disclosure occurs, ALG takes reasonable steps to ensure information is handled in accordance with the Australian Privacy Principles or equivalent privacy protections.

By enrolling with ALG, students acknowledge that some personal information may be disclosed to overseas recipients or accessed through overseas-based systems and service providers for the purpose of delivering education and support services, maintaining student records, regulatory reporting or operating ALG systems and platforms.

ALG does not adopt, use or disclose government-related identifiers as its own identifiers for individuals except where authorised or required by law.

5.3 Website, Analytics and Online Systems

ALG websites and online systems may use cookies, analytics tools and related technologies to:

- improve website functionality
- monitor usage patterns
- support website and system security
- improve student services and online user experience.

ALG may use third-party analytics services such as Google Analytics to analyse website usage and improve online services. ALG websites may also include interfaces with social media platforms. Individuals accessing or interacting with these services should refer to the privacy policies of those third-party providers.

Individuals may adjust browser settings to disable cookies, however some website functions may be affected.

5.4 Data Security and Storage

ALG maintains physical, administrative and technical safeguards to protect student personal information from misuse, interference, loss, unauthorised access, modification or disclosure. These safeguards may include:

- secure servers and systems
- password protections and user access controls
- encryption and secure online platforms
- restricted staff access
- secure storage locations
- controlled disposal and destruction processes.

ALG stores student information only for as long as required under applicable legislation, regulatory obligations and record retention requirements.

Where records are no longer required, ALG takes reasonable steps to securely destroy or permanently de-identify the information.

5.5 Privacy Incidents and Data Breaches

ALG will respond promptly to actual or suspected privacy incidents and data breaches to minimise risks to individuals, protect personal information and support compliance with applicable privacy obligations.

ALG will investigate, manage and respond to privacy incidents in accordance with this Policy and Procedure, the **Data Breach Response Policy and Procedure**, and applicable legislative requirements.

5.6 Notifiable Data Breaches and Reporting Obligations

ALG will assess all actual or suspected privacy incidents and data breaches promptly to determine whether notification obligations apply under the Privacy Act 1988 (Cth) and the Notifiable Data Breaches (NDB) scheme. In assessing an incident, ALG may consider:

- the nature and sensitivity of the information involved
- the number of individuals potentially affected
- whether the information has been accessed, disclosed, lost or compromised
- the likelihood that serious harm may occur to affected individuals
- whether remedial actions can reduce or eliminate the risk of harm.

Where an incident is determined to be an eligible data breach, ALG will:

- notify the Office of the Australian Information Commissioner (OAIC) as soon as practicable where required by law
- notify affected individuals where required
- document the incident, assessment findings and actions taken
- implement corrective and preventative actions to reduce the likelihood of recurrence
- record actions in relevant registers and continuous improvement processes where appropriate.

Where an incident does not meet notification thresholds, ALG may still investigate, document and implement corrective actions where appropriate.

5.7 Access and Correction of Personal Information

All ALG stakeholders including students s may request access to or correction of personal information held by ALG in accordance with the Privacy Act 1988 (Cth) and Australian Privacy Principle 12 (Access to Personal Information).

Requests for access must:

- be made in writing
- provide sufficient information to identify the records requested
- allow ALG to verify the identity of the individual making the request.

ALG will take reasonable steps to provide access to personal information requested by the individual within a reasonable timeframe and in a suitable format where practicable.

Access may be refused, limited or redacted where permitted by law, including where:

- providing access would unreasonably impact the privacy of another individual
- the information relates to existing or anticipated legal proceedings
- the information is subject to legal professional privilege
- the request is frivolous or vexatious
- the information cannot reasonably be separated from third-party information
- refusal is otherwise authorised or required by law.

Where access is refused or limited, ALG will provide written reasons for the decision and information about available complaint pathways where required by law.

ALG may provide access through copies of records, supervised inspection, summaries or redacted documents where appropriate.

5.8 Privacy Complaints

Individuals may make a privacy-related complaint where they believe personal information has been mishandled or privacy obligations have not been met.

Privacy complaints are managed in accordance with the **Complaints and Appeals Policy and Procedure.**

ALG will:

- acknowledge privacy complaints promptly
- investigate the matter fairly and confidentially
- aim to provide a written outcome within 30 calendar days where practicable
- maintain records of complaints and outcomes in the Complaints Register.

Individuals who are dissatisfied with ALG's handling of a privacy complaint may contact the Office of the Australian Information Commissioner (OAIC) for further information or to make an external privacy complaint.

6. Procedure

Step	Key Actions	Responsibility	Supporting documentation
1. Collection of Personal Information	• Collect student personal information through application and enrolment forms, online portals, websites, student management systems, telephone conversations, email	Admissions Team	Application forms Student Management

	communications, direct interactions with students and, where reasonably necessary, from authorised third parties or publicly available sources. • Where information is provided by third parties (e.g. education agents), record the source of the information and inform the student that the information has been provided.		System (RTOM) records Agent documentation
2. Types of Information Collected	• Collect only information necessary to administer enrolment and training services. • Record student personal details including name, date of birth, gender, contact details, identification documents, enrolment information, academic progress, attendance records and fee payment information. • Where relevant, record medical or support information voluntarily provided by the student. • For international students, also collect nationality, passport details, visa information, OSHC details, English language test results and course commencement and completion information.	Admissions Team	Student files Enrolment documentation Visa and identification records
3. Providing Privacy Notices	• Provide students with the NCVER Privacy Notice and relevant ALG privacy information as part of the Letter of Offer and Student Agreement process before enrolment is finalised. • Inform students about why their personal information is collected, how it may be used and disclosed, and how students may request access, correction or make a privacy complaint.	Admissions Team	Letter of Offer and Student Agreement NCVER Privacy Notice
4. Use of Personal Information	• Use student personal information only for legitimate operational purposes. • Use information to administer enrolments, deliver training and assessment, issue AQF certification documentation, provide student support services, communicate with students, conduct surveys and continuous improvement activities, and meet government reporting obligations.	Administration Team	Student records Survey data Certification records
5. Disclosure of Personal Information	• Disclose student personal information only where authorised. • Provide required information to government agencies, NCVER, ASQA, the Tuition Protection Service and other authorised bodies where reporting obligations apply. • Where relevant, share information with other education providers for	Compliance Team	Government reporting records NCVER (VETMISS) submissions Correspondence

	credit transfer or pathway purposes or with employers where training is employer-funded. • Do not disclose personal information to other third parties without the student's consent unless disclosure is required or authorised by law.		
6. Access and Correction of Personal Information	• Assess requests for access to personal information in accordance with the Privacy Act 1988 (Cth) and Australian Privacy Principle 12. • Verify the identity of the individual before releasing information. • Review records to identify whether any information should be withheld, limited or redacted where permitted by law, including information affecting the privacy of other individuals or information subject to legal privilege. • Provide access through copies, supervised inspection, summaries or redacted records where appropriate. • Where access is refused or limited, provide written reasons and information regarding available complaint pathways.	Administration Team Quality Assurance Team	Written requests Student records Privacy Act 1988 (Cth) OAIC guidance materials Access request correspondence
7. Data Security and Storage	• Store student personal information securely in the student management system and authorised records storage locations. • Restrict access to authorised staff only. • Ensure hard copy records are stored in secure cabinets or controlled storage areas. • Dispose of records securely when they are no longer required in accordance with record retention requirements.	Administration and IT Teams	Information Management Systems Disposal records
8. Privacy Incidents and Data Breaches	• Record actual or suspected privacy incidents immediately • Escalate incidents to Quality Assurance and relevant management personnel. • Assess the incident and determine whether it may constitute an eligible data breach under the Privacy Act in accordance with the Data Breach Response Policy and Procedure. • Notify the OAIC and affected individuals where notification requirements apply. • Record actions taken and implement corrective actions where required. • Record actions within relevant registers and continuous improvement processes where appropriate.	Quality Assurance Team IT Team and Management	Data Breach Response Policy and Procedure Incident reports, Data Breach Register, OAIC online form , Continuous Improvement Register
9. Privacy Complaints	• Accept privacy-related complaints from students in accordance with the	Student Services & QA Team	Complaint Form

	Complaints and Appeals Policy and Procedure. • Record the complaint in the Complaints Register, investigate the matter and respond to the student within the timeframe specified in the Complaints and Appeals procedures. • Acknowledge privacy complaints promptly and aim to provide a written outcome within 30 calendar days where practicable.		Complaints Register

7. Related Documents

This policy should be read in conjunction with:

- Complaints and Appeals Policy and Procedure
- Enrolment Form
- Letter of Offer and Student Agreement
- Complaints Form
- Complaints Register
- Student Management System
- NCVER Privacy Notice
- Incident Report Form
- Data Breach Register
- Data Breach Response Policy and Procedure
- Office of the Australian Information Commissioner (OAIC)

8. Document Information and Review

Document Information		
Document ID	STU-01	
Policy Category	STU - Student Administration & Support	
Responsible officer	Joe Lynch	
Key Stakeholder(s)	All ALG Stakeholders	
Approval by	CEO	
Endorsed by	Academic Director and Head of Quality Assurance	
Date of Approval	21/05/2026	
Date Effective	12/06/2026	
Date of Next Review	21/05/2027	
Version History		
Version	**Date**	**Amendment(s)**
1.0	09 March 2026	• Created as a separate document from information provided in Student Handbook