Privacy Policy

1. Purpose

RTO Connect Pty Ltd t/a Australian Study Link Institute hereinafter referred as ASLI is committed to providing quality training and assessment in accordance with the Standards for Registered Training Organisations (RTO Standards 2025). ASLI is required to comply with the Privacy Act 1988 including the Australian Privacy Principles (APPs), and relevant obligations under the ESOS Act 2000 and the National Code 2018 (Standard 3.3.6).

This policy outlines how ASLI collects, uses, stores, and discloses personal information of its students, staff, and stakeholders. ASLI is committed to protecting personal information and ensuring it is only used for its primary purpose (i.e., enrolment, education delivery, support services, and compliance with legal obligations).

Personal information may be shared with:

- The Department of Education
- The Department of Home Affairs
- The Tuition Protection Service (TPS) as required under the ESOS Act 2000 and the National Code 2018.

ASLI will ensure the following:

- Maintains and provides a current Privacy Policy.
- Collects personal information fairly and lawfully, for enrolment and operational purposes.
- Information will not be disclosed to third parties without written consent, unless required by law.
- Records are securely stored, both in digital and physical formats.
- Students are informed of their privacy rights during pre-enrolment and orientation, in line with National Code 2018 Standard 2, 3 and 6
- Individuals have the right to access and correct their personal information in accordance with APPs 12 and 13. Requests must be made in writing to the Campus Manager or Training Manager.
- Reasonable steps are taken to protect information from loss, misuse, unauthorised access, modification, or disclosure.

The thirteen (13) Australian Privacy Principles are:

- Australian Privacy Principle 1 - Open and transparent management of personal information
- Australian Privacy Principle 2 - Anonymity and pseudonymity
- Australian Privacy Principle 3 - Collection of solicited personal information
- Australian Privacy Principle 4 - Dealing with unsolicited personal information

- Australian Privacy Principle 5 - Notification of the collection of personal information
- Australian Privacy Principle 6 - Use or disclosure of personal information
- Australian Privacy Principle 7 - Direct marketing
- Australian Privacy Principle 8 - Cross-border disclosure of personal information
- Australian Privacy Principle 9 - Adoption, use or disclosure of government related identifiers
- Australian Privacy Principle 10 - Quality of personal information
- Australian Privacy Principle 11 - Security of personal information
- Australian Privacy Principle 12 - Access to personal information
- Australian Privacy Principle 13 - Correction of personal information

2. Scope

This policy applies to all students, staff contractors and any individuals involved with ASLI. The collected information will be either in electronic or in hard copy format. This includes information collected before, during, and after enrolment, in accordance with the ESOS Act 2000, National Code 2018 (Standard 3.3.6), and the Privacy Act 1988.

3. Responsibility

CEO, Campus Manager and Training Manager will be responsible for implementation and monitoring of this policy and will ensure that all staff members are aware of this policy and its underpinning legislative requirements and comply with it all the times. ASLI will take privacy issues seriously and will stay committed to protect the privacy of individuals. This includes personal, health, financial and other confidential information which is necessary for ASLI to carry out its functions. Training on privacy obligations and data handling procedures will be provided to staff as part of ASLI's onboarding and compliance processes.

4. Policy Principles

4.1. Legislation

ASLI is legally required to comply with the Privacy Act 1988, including the Australian Privacy Principles (APPs) The Privacy and Other Legislation Amendment Act 2024 (most provisions commenced 10 December 2024; the statutory tort for serious invasions of privacy commenced 10 June 2025) strengthened the OAIC's enforcement powers and clarified data security obligations. ASLI ensures all data practices align with these updated requirements.

4.2. Underpinning Principles

Personal Information is defined in the Privacy Act 1988 to mean "information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not

Sensitive Personal Information is defined in the Privacy Act 1988 to mean "information or an opinion about an individual's" that is also personal information, such as:

- racial or ethnic origin; or
- political opinions; or
- membership of a political association; or
- religious beliefs or affiliations; or
- philosophical beliefs; or
- membership of a professional or trade association; or
- membership of a trade union; or
- sexual orientation or practices; or
- criminal record; or health information, genetic information.

4.3. Website Privacy and Cookies

ASLI's website may use cookies or similar tracking technologies to improve user experience, gather anonymous website analytics, and assist with functionality. By continuing to use the website, users consent to the use of cookies where applicable. Personal information is only collected via online forms or portals where users voluntarily provide it. Users can manage cookie settings through their internet browser. No sensitive information is collected through ASLI's website unless users provide it voluntarily and explicitly. All website data collection complies with the Privacy Act 1988 and the Australian Privacy Principles.

5. Procedures

5.1. Consideration of the Privacy/ Managing Personal Information

ASLI endeavours to balance the rights of privacy with the need to be accountable and transparent in its dealings. ASLI manages student's personal information by:

- Ensuring that personal information is managed in an open and transparent way.
- Take reasonable steps to implement practices and procedures that will facilitate dealing with enquiries or complaints from individuals regarding compliance with the Australian Privacy Principles (APPs).
- Ensure that it maintains an up-to-date policy about the management of personal information.

- Ensure that Privacy Policy contains the following information:
  i. The kind of information that is collected and held
  ii. How the information is collected and held
  iii. The purposes for which information is collected, held, used and disclosed
  iv. How an individual may access their personal information that is held by and seek correction of such information as necessary
  v. How the individual may make a complaint about a breach of the APPs and how ASLI will deal with the complaint, refer to the Feedback, Complaints and Appeals policy on ASLI's website.
  vi. Whether ASLI is likely to disclose personal information to overseas recipients, and if so the countries in which such are likely to be located.
  vii. Provide the Privacy Policy free of charge and in such form as appropriate, and as is reasonable.
  viii. Access to the Privacy Policy by all students (including overseas students) during pre-enrolment and orientation, as required under National Code 2018 Standard 2, 3 and 6.
  ix. Compliance with RTO Standards 2025 and ESOS Act 2000 in managing all personal and sensitive information.
  x. Integration of changes introduced by the Privacy and Other Legislation Amendment Act 2024, and compliance with the Notifiable Data Breaches scheme.

5.2. Anonymity and Pseudonymity

ASLI respects that individuals may not wish to identify themselves when making enquiries on products and services; however, ASLI requires full personal details as required by law and for identification purposes from clients. This includes but is not limited to requirements under the ESOS Act 2000, National Code 2018, and RTO Standards 2025, which mandate accurate identification for enrolment, visa compliance, and issuance of nationally recognised qualifications and reporting via PRISMS.

5.3. Collection and Use of Personal Information

ASLI will not collect personal information from you unless that information is necessary for one or more of its functions or activities or is required by law. ASLI advises that it is required by law to collect, hold, use and supply personal information, in accordance with the National VET Provider Collection Data Provision Requirements. Any information supplied by students to ASLI will only be used to provide information about study opportunities, to enable efficient administration, and to maintain proper academic records. Only authorised personnel will have access to this information.

All information collected is governed by the Australian Privacy Principles (APPs), as amended by the Privacy and Other Legislation Amendment Act 2024. This includes information necessary for the delivery of vocational education and training services, for compliance with RTO Standards 2025, ESOS Act 2000 and National Code 2018, and for reporting to the Department of Education, the Tuition Protection Service (TPS), and other government agencies where required by law.

ASLI will take reasonable steps at or before the time of collection to ensure that you are aware of:

- Who we are and how to contact us
- How to gain access to your own information
- The purpose for which the information is being collected
- Any organisation to which we would normally disclose information of that kind
- Any law that requires the particular information to be collected
- The main consequences for the individual if all or part of the information is not provided.
- Your rights under the Privacy Act 1988, including rights to access and correct your personal information (APPs 12 and 13) and to complain about a breach of the Australian Privacy Principles.

ASLI collects information from you in the following ways:

- When you register your interest online, apply for enrolment, request certain services or products, or otherwise contact or do business with us.
- Information may be collected from enrolment forms, certified documents, telephone calls, faxes, emails, letters sent by you.
- Information may be collected from third parties, such as other training providers, regarding confirmation of training and ongoing professional development that you have attended, as permitted by you.
- Should ASLI collect information about you from a third party we will take reasonable steps to ensure that the individual is or has been made aware of the matters listed above except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual. unless doing so would pose a serious threat to the life, health or safety of an individual, in accordance with APP 3.6(b).

5.4. Dealing with Personal Information

ASLI will act lawfully and in a fair and nonintrusive way. ASLI will ensure that the personal information that it collects is accurate, up to date, complete and relevant.

ASLI will not use or disclose personal or sensitive information for any purpose other than what it was collected for, unless the relevant person has provided written consent to use or disclose that information in circumstances that are different to those for which it was collected. The circumstances where an exception may occur are:

- Where the use or disclosure of this information is required or authorised by or under an Australian law or a court/tribunal order
- The individual would reasonably expect to use or disclose the information for the secondary purpose
- A permitted health situation exists in relation to the use or disclosure of the information by ASLI
- A permitted general situation exists in relation to the use or disclosure of the information by ASLI
- ASLI reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.
- ASLI will document any secondary use or disclosure decisions in accordance with its internal compliance framework.

ASLI collects your personal information so as to:

1. Process applications
2. Manage your enrolment
3. Record and maintain your details
4. Administering training programs
5. Record and maintain details of your ongoing training and assessment
6. Provide you with details regarding client services, benefits, and training opportunities
7. Notify you about upcoming events and opportunities
8. Gain feedback from you
9. Communicate with you
10. Report to relevant authorities as required by law.

All uses and disclosures will be governed by secure record-keeping practices, with access restricted to authorised personnel, in compliance with APP 11, RTO Standards 2025, and ASLI's internal data security procedures.

Digital data will be protected through encrypted platforms and role-based access permissions. Physical records will be stored in locked, access-controlled environments.

5.4.1.Direct Marketing

ASLI may use personal information (specifically your name and relevant address details) and information about your preferences for direct marketing (i.e. the communication channels which you prefer for receiving direct marketing from us and the types of products and services in which you are interested in) so as to let you know about our services and benefits, where we have your written consent.

ASLI will also provide an opt-out and/or unsubscribe method that is easily accessible for individuals to request not to receive direct marketing communications. ASLI will action all opt-out requests within a reasonable time (As per Standards for RTO 2025) and will not send further marketing without consent.

5.4.2.Cross Border Disclosure

ASLI does not disclose personal information to overseas recipients unless prior written approval is received by the individual who the personal information relates. Where disclosure is required for compliance with the ESOS Act 2000 or reporting to international education-related bodies, ASLI will ensure the receiving party upholds privacy protections substantially similar to the Australian Privacy Principles, in accordance with APP 8.1 and RTO Standards 2025.

Where consent cannot be obtained, ASLI will rely on the exceptions outlined in APP 8.2 (e.g. disclosure required by law or for a permitted general situation) and document this accordingly. For more information refer to: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information

5.4.3.Adoption, use or Disclosure of Government Related identifiers

It is required by law (Student Identifier Act 2014) to collect, maintain and report to relevant Government agencies the individual's Unique Student Identifier (USI) number in accordance with the National VET Provider Collection Data Provision Requirements. This information may be shared with:

- Commonwealth and State/Territory government departments and agencies and statutory bodies performing functions relating to VET for:
    - The purpose of administering and auditing VET, VET providers and VET programs
    - Education related policy and research purposes; and
    - To assist in determining eligibility for training subsidies
- VET regulators to enable them to perform their VET regulatory functions
- VET admissions Bodies for the purpose of administering VET and VET programs,
- Current and former Registered Training Organizations to enable them to deliver VET courses to the individual, meet their reporting obligations under the VET standards and government contracts and assist in determining eligibility for training subsidies
- The Department of Education, the Department of Home Affairs, or the Tuition Protection Service (TPS), where required under the ESOS Act 2000 or National Code 2018.

ASLI will not disclose the Unique Student Identifier (USI) number for any other purpose, including on AQF certification documentation (e.g., testamurs, statements of attainment, or Record of Results)

ASLI must not adopt the Unique Student Identifier (USI) number as its own identifier of the individual. USI data will be stored securely, encrypted where applicable, and only accessible to authorised personnel in accordance with the Privacy Act 1988, APP 9, and RTO Standards 2025.

5.4.4.Payment details/Credit Card Authorisation

In circumstances, where the student chooses to make payments using a credit card, they may do so only upon filling the credit card authorisation form. The authorisation form is viewed and processed by the Administration department.

Campus Manager upon processing the payment, secures the information in a locked cabinet which is in turn placed in a secured room. Only Campus Manager will have the key access to the room and the cabinet. Electronic storage of credit card details is strictly prohibited unless encrypted, access-controlled, and compliant with the Payment Card Industry Data Security Standard (PCI DSS) and APP 11 of the Privacy Act 1988.

The credit card authorisation form is retained only for the length of the course enrolment plus one year, post which they must be destroyed by document disposal professionals. A corresponding entry of the disposal needs to be maintained in the document disposal register. Destruction must be conducted in a manner that prevents unauthorised recovery or reconstruction of data, in line with RTO Standards 2025, APP 11, and ASLI's Records Management Policy.

Refer to: "Records Management Policy" for detailed retention and destruction guidelines.

5.5. Integrity of Personal Information

ASLI will take steps, as are reasonable, to ensure that the personal information it:

- Collect is accurate, up to date and complete.
- Uses or discloses, is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

This includes regular verification and updating of student records, particularly when personal contact details, visa-related information, or emergency contacts have changed.

5.6. Security Of Personal Information

ASLI will take steps, as are reasonable in the circumstances to:

- Protect the information from misuse, interference and loss as well as unauthorised access, modification or disclosure.
- Ensure that personal information is securely destroyed or de-identified when it is no longer required, in accordance with APP 11.2 and Records Management Policy
- Wherever possible, it will collect information directly from its students rather than from third parties.

ASLI will also implement appropriate physical and digital security controls, including:

- Role-based access restrictions
- Data encryption at rest and in transit
- Multi-factor authentication (MFA)
- Secure storage (e.g., locked cabinets for physical records)

These controls apply to all personal and sensitive data and are implemented in accordance with the Privacy Act 1988, RTO Standards 2025, and Australian Cyber Security Centre (ACSC) recommendations.

5.6.1. Data Breach Response Plan:

ASLI has a documented Data Breach Response Plan in line with the Notifiable Data Breaches (NDB) scheme under the Privacy Act 1988. In the event of an eligible data breach likely to result in serious harm to any individual, ASLI will notify the affected individuals and report the breach to the Office of the Australian Information Commissioner (OAIC) as soon as practicable after forming reasonable grounds to believe an eligible data breach has occurred. Where ASLI only suspects an eligible data breach, it will take all reasonable steps to complete an assessment within 30 calendar days after becoming aware of the grounds for suspicion. All staff are trained to recognise and respond to data breaches, and actions will be documented in accordance with ASLI's incident management procedures.

ASLI's response plan includes:

- Containment and assessment of the breach
- Risk evaluation to determine if serious harm is likely
- Notification to affected individuals and the OAIC if harm is likely
- Review of the breach cause and prevention of recurrence
- Internal logging and reporting of all breaches, including near misses, even if not notifiable

Refer to ASLI's data breach response plan which can be collected from reception if required.

5.7. Disclosure of Personal Information

Personal information about student(s) studying with ASLI may be shared with Australian Government and regulators (including ASQA and the Department of Education). This information includes personal and contact details, course enrolment details and changes and, for international students, the circumstances of any suspected breaches of the student's visa conditions.

ASLI will not disclose any personal information of a student, except as permitted under these policies. ASLI will not disclose personal information to a person, body or agency (other than the individual concerned) unless:

- The individual concerned has expressly or implicitly consented to the disclosure in writing; or

- The person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious threat to the life or health of the student or of another person; or
- The disclosure is required or authorised by or under law; or
- 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, or for the protection of the interests of the government, statutory authority or statutory office holder as an employer; or
- The disclosure is necessary for the performance of ASLI's functions as a registered training organisation and/or CRICOS provider, in accordance with its reporting obligations to relevant authorities such as the Department of Education, Department of Home Affairs, ASQA, and TPS.

ASLI will disclose information for the purpose of the protection of public revenue. ASLI will include a note of the disclosure in the record containing that information. Personal information may be shared with other Colleges where students enrol or apply to enrol.

In case of work-based training components ASLI may require notifying Host Organisation (including approved entity, serviced providers of employer, agents or their authorised contractors) of any concerns, issues or opportunities relating to the practical placement, including student course progression.

All disclosures will be made in line with APP 6 and RTO Standards 2025 Outcome Standard 3.3 to ensure the security and lawful use of personal information.

5.8. Access to and Correction of Personal Information

A student may access their own personal information held by ASLI at no charge. Individuals will be advised of how they may access or obtain a copy of their personal information within 30 days of receiving the individual's written request or as soon as practicable.

ASLI allows students to apply for and receive personal information that ASLI holds about students according to the above requirements. The request should be lodged in writing, addressed to the Campus Manager, providing full details of the student's name, ID number and details of the specific information required. ASLI ensures that these processes comply with the Privacy Act 1988 and RTO Standards 2025.

However, in some circumstances, ASLI may not permit access to individuals for their personal information. If this is ever the case, ASLI will provide full details for the legal reasons for this decision. These may include that believes:

- That giving access to the information would pose a serious threat to the life, health or safety of the individual, or to public health or public safety; or
- Giving access would have an unreasonable impact on the privacy of other individuals; or
- The request for access is frivolous or vexatious; or

- The information relates to existing or anticipated legal proceedings between and the individual, and would not be accessible by the process of discovery in those proceedings; or
- Giving access would reveal the intentions of in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- Giving access would be unlawful; or
- Denying access is required or authorised by or under an Australian law or a court/tribunal order; or
- ASLI has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
- Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- Giving access would reveal evaluative information generated within in connection with a commercially sensitive decision-making process.

ASLI will not charge a fee for access to personal information. The exception is re-prints of certification documentation previously supplied.

6. Requests for Erasure or Data Portability

The Privacy Act 1988 does not currently give individuals a general right to erasure or data portability (these were not enacted in the 2024 reforms). ASLI will respond to any such request under APP 11.2, APP 12 and APP 13 and its record-retention obligations. Personal information that ASLI no longer needs and is not required to retain by law (including under the ESOS Act 2000, the National Code 2018 and the Standards for RTOs 2025) will be destroyed or de-identified under APP 11.2.

ASLI will make all reasonable efforts to ensure that personal information recorded by ASLI is up to date. If a student believes that the personal information retained by ASLI is out of date or otherwise misleading or inaccurate, the student may request that ASLI amend his or her personal information. ASLI will amend the information, if it is found that the information is out of date, misleading or inaccurate.

If ASLI corrects and updates personal information about an individual that ASLI previously disclosed to another education provider and the individual requests the Institute (ASLI) to notify the other provider of the correction, then ASLI will take steps that are reasonable in the circumstances, to provide that information unless it is impractical or unlawful to do so.

Where personal information relates to all students, ASLI will also notify Department of Home Affairs to ensure visa records are accurate, in line with ESOS Act 2000 and National Code 2018.

If ASLI refuses to correct the information as requested by the individual, ASLI will give a written notice to a student that sets out:

a) the reasons for the refusal; and
b) the mechanisms available to complain about the refusal; and
c) any other matter prescribed by the regulations.

With regard to the correction of personal information held:

ASLI should be satisfied that information is inaccurate, out of date, incomplete, irrelevant or misleading, ASLI will take such steps as reasonable to correct the information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading. ASLI will not charge students for making the request, for correcting the personal information or for associating the statement with the personal information. All updates will be logged securely, with version control if applicable, in compliance with the Privacy Act and RTO Standards 2025.

7. Records Management

All personal information and records are maintained in accordance with Records Management Policy. (See Records Management Policy)

8. Monitoring and Improvement

All Privacy practices are monitored by the CEO and areas for improvement identified and acted upon. (See Quality Management Policy and Procedures). Monitoring includes audits of access controls, security incidents, and legislative updates. Identified risks or breaches are managed through the continuous improvement system.

Findings from internal reviews and breach responses are used to inform updates to the Privacy Policy and Records Management procedures. Annual reviews ensure alignment with current legal obligations, including any future amendments to the Privacy Act.

9. Complaints

Students have the right to complain if they believe that believe their privacy has been breached. If a student is not satisfied with ASLI's response within 30 days, they may lodge a complaint with the Office of the Australian Information Commissioner (OAIC): www.oaic.gov.au, phone 1300 363 992. Students can access Feedback, Complaints and Appeals policy available on ASLI's website or can contact students support office. All complaints will be managed in line with National Code 2018 Standard 10.2, RTO Standards 2025, and ASLI's Feedback, Complaints and Appeals Policy. ASLI will ensure complaints are handled confidentially, fairly, and resolved within the reasonable timeframe. ASLI will also document privacy-related complaints in its incident register and ensure outcomes are reviewed as part of the continuous improvement process.

10. Version Control and Review

This Privacy Policy is reviewed annually or earlier if legislative or regulatory changes occur. Reviews will consider any changes to the Privacy Act 1988, including reforms, and update policy wording, procedures, and staff training materials accordingly.