Personal Information & Privacy Policy

1. Purpose

We collect and manage your personal information with respect, integrity, and in line with Australian privacy law. This policy explains:

- What information we collect about you
- Why we collect it
- How we use, store, and protect it
- Who we might share it with
- How you can access or correct it
- What happens if there is a data breach

2. Definitions

- **Personal Information**: Any information that identifies you or could identify you (e.g., name, address, photos, student record).
- **Sensitive Information**: Special categories of data (like health or criminal history). We only collect these when absolutely needed, and usually with your written consent.

3. Who This Policy Applies To

This policy covers:

- Students
- Staff
- Contractors
- Visitors

All personal information collected by AIAC is covered under this policy, whether collected on paper, digitally, in conversation, or during training.

4. Laws & Standards We Follow

We comply with:

- Privacy Act 1988 and the Australian Privacy Principles (APPs)
- The Standards for RTOs 2025
- Student Identifiers Act 2014
- Any relevant aviation or regulatory laws

5. What Information We Collect

We only collect what is necessary, for example:

- Identity (passport, driver's licence, USI, etc.)
- Training records (enrolment, assessments, logbooks)
- Safety or medical information (if required)
- Employment details (for staff)
- Marketing data (with your consent. e.g., photos, website analytics)

6. How We Collect It

We collect information:

- Directly from you (forms, interviews)
- From your agent or authorised representative
- From other parties (CASA, exam bodies, previous employers)
- In some cases, we might collect info without explicit notice (e.g., for safety) only when reasonable or legally required

7. Your Consent

Consent for Collection and Use

We will always ask for your consent when we collect sensitive information or optional information (such as photos, testimonials, or medical details not required by law). Consent may be given in writing, electronically, or through signed forms.

How Consent Is Stored

All consent forms are stored securely in your student or staff file and recorded in our internal consent register. Only authorised staff can access these records.

Withdrawing Consent

You may withdraw your consent at any time by emailing the Office Manager. Withdrawal will not affect any use of your information that was required by law or already completed.
If you withdraw consent, we will stop using that information and securely destroy or de-identify it where possible.

8. What If You Want to Stay Anonymous?

Where possible, you can choose not to identify yourself, but sometimes certain information

(like licensing, USI, or medical records) is required. If you don't provide mandatory information, we may not be able to enrol you or deliver certain services.

9. What If You Don't Provide Information?

If you withhold critical information:

- We might refuse your enrolment
- You may not be able to fly / train / assess
- You may not be eligible for licences or medicals
- We might not be able to process complaints or safety concerns
- Payroll or visa processes could be impacted

10. How We Use Your Information

We use your personal information for:

- Training, assessing, and supporting you
- Booking exams (CASA, ASPEQ)
- Monitoring your academic progress, safety, and compliance
- Regulatory reporting (ASQA, CASA, NCVER, Home Affairs)
- Marketing (but only with your consent)

11. Who We Might Share Your Information With

We share only what is necessary and only with:

- Government bodies (CASA, ASQA, NCVER, Home Affairs)
- Law enforcement or health services (if needed)
- External contractors (e.g., exam providers)
- Marketing partners (only with your permission)

All third parties must comply with relevant privacy laws.

12. How We Store & Protect Your Information

We store your information securely:

- Electronically (password protected, restricted access)
- Physically (locked cabinets for hard-copy files)
- With regular backups and security measures to prevent loss, unauthorised access, or misuse

Some cloud systems we use may store information overseas. We take reasonable steps to ensure these providers comply with privacy laws and protect your information to the standards required under the Australian Privacy Principles.

13. How Long We Keep Records

We keep your records for the legally required minimum periods. See the Data Protection Policy for more information.

14. If There Is a Data Breach

We comply with the Notifiable Data Breaches Scheme (NDB Scheme). A notifiable data breach occurs when:

- Personal information is lost or accessed/disclosed without authorisation, **and**
- This is likely to cause serious harm to an individual.

If a notifiable breach occurs, we will:

1. Contain the breach immediately
2. Assess the level of harm
3. Notify affected individuals as soon as practicable
4. Notify the OAIC where legally required
5. Take action to prevent future breaches

If you have a concern about how your personal information has been collected, used, or shared, you may lodge a privacy complaint at any time. Privacy complaints follow the same process as our Complaints and Appeals Procedure.

15. Access & Correction

You have the right to:

- See the personal information we hold about you
- Ask us to correct any mistakes

Before we release or update personal information, we must verify your identity. This helps protect your privacy and prevent unauthorised access. If identity cannot be verified, access will not be provided.

Acceptable verification includes:

- Photo ID (student card, driver's licence, passport)
- Security questions
- Verification through your enrolled email address or student portal

16. Marketing & Media

We will only use your personal information for marketing if you give us written permission by completing our **Media Release Consent Form** (available in your written agreement).

17. Responsibilities

- **Student:** Provide accurate info, update us when things change, know your privacy rights
- **All Staff**: Handle data respectfully, follow procedures, report any data breaches
- **Compliance Officer**: Oversee privacy compliance, keep policies up to date, manage third-party relationships

18. Related Documents

- Data Protection Policy
- Media Release Consent Form
- Complaints & Appeals Procedure
- Student Handbook
- USI Privacy Notice