



ACIMSolutions

Australian Centre for Investigation, Incident & Management Solutions

Privacy Policy and Procedures

1. PURPOSE

This policy explains how ACIM Solutions (ACIMS) maintains compliance with relevant legislative requirements, including the Australian Privacy Principles, when collecting, using, disclosing and otherwise handling personal information relating to individuals. This includes information available to staff, individuals and other third parties with whom ACIMS interacts.

2. POLICY STATEMENT

ACIMS is committed to maintaining the privacy and confidentiality of its clients and staff records. ACIM Solutions complies with the Privacy Act 1988 including Australian Privacy Principles as found in the Privacy Amendment (Enhancing Privacy Protection) Act 2012. ACIMS manages personal information in an open and transparent way and provides staff with suitable procedures to manage related inquiries and complaints.

3. SCOPE OF POLICY

This policy applies to all staff, individuals and third parties with whom ACIMS interacts and where personal information is collected, retained, used or shared.

4. POLICY PRINCIPLES

4.1. MANAGING PERSONAL INFORMATION

4.1.1. Purposes for information collection, retention, use and disclosure

ACIMS retains a record of personal information about all individuals with whom we undertake any form of business activity. There are certain reasons why we must collect, hold, use and disclose information, e.g.

- providing services to clients
- managing staff and contractors
- promoting products and services
- conducting internal business functions and activities.

Some information is gathered in accordance with the National Vocational Education and Training Regulator (Data Provision Requirements) Instrument 2020, which requires all Registered Training Organisations to collect data from students in accordance with the Australian Vocational Education and Training Management Information Statistical Standard (AVETMISS).

ACIMS may disclose information held on individuals for valid purposes to a range of entities including governments (Commonwealth, State or Local); and employers (and their representatives). This data will be de-identified as appropriate and allowable.

ACIMS will not use personal information in external AI systems without prior consent of students.

4.1.2 Kinds of personal information collected and held

The following types of personal information are collected, depending on the need for service delivery:

- contact details
- employment details

- product/service progress and achievement information
- financial billing information

The following types of sensitive information may also be collected and held:

- identity details
- complaint or issue information.

4.1.3 Collection of personal information

Where possible ACIMS prefers to collect required personal information directly from the individuals concerned. This may include the use of forms (such as enrolment forms) and the use of web-based systems (such as online enquiry forms, web portals or internal operating systems).

ACIMS may receive some information via third party sources in undertaking service delivery activities. This may include information from governments (Commonwealth, State or Local), employers and their representatives, and sub-contractors who interact with individuals in their roles relating to service delivery and compliance.

4.1.4 Storage of personal information

ACIMS usual approach includes suitable measures to ensure personal information is held securely. Where possible, information is:

- stored electronically (if paper based, converted to electronic means as soon as practical)
- stored in secure, password protected systems, such as financial and student management system
- monitored for appropriate authorised use.

Only authorised personnel are provided with login information to each system, with system access limited to only those relevant to their specific role. ACIMS computer systems are virus protected, backed up and access is monitored. Individual information held across systems is linked through ACIMS allocated identification number for the individual (student ID).

4.1.5 Retention and destruction of information

ACIMS has a Records Management Policy which details the periods for which personal information records must be kept. This is in alignment with general government guidance and requirements such as the Standards for Registered Training Organisations, that require certain information be kept for 30 years. Destruction of paper-based records occurs as allowable by electronic storage and our Records Management Policy. Documents are destroyed appropriately and securely.

4.1.6 Accessing and seeking correction of personal information

ACIMS confirms all individuals have a right to request access to their personal information held and to request its correction at any time. A number of authorised third parties, other than the individual, may also request access to an individual's personal information.

Individuals or third parties may at any stage request that their records held by ACIMS relating to their personal information be updated. Upon this request, ACIMS will correct personal information held and notify any third parties of corrections made to personal information, if this information was previously provided. The procedure to access and correct personal information is detailed at the end of this policy.

4.1.7 ACIMS initiated correction of personal information

ACIMS takes reasonable steps to correct personal information we hold in cases where we believe the personal information held is inaccurate, out-of-date, incomplete, irrelevant or misleading. This awareness may occur through collection of updated information, in notification from third parties or through other means.

4.1.8 Complaints about a breach of privacy

If an individual feels that ACIMS may have breached their privacy or this policy, the procedure to complain is detailed at the end of this policy. This includes concerns about use of personal or sensitive information in AI systems.

4.1.9 Likely overseas disclosures

ACIMS confirms that individuals' personal information will not be disclosed to overseas recipients other than in the course of general cloud hosting requirements of the ACIMS Student Management System or other cloud storage solutions. Varied overseas locations may be used as part of reputable cloud hosting services for provision of portal services.

4.1.10 Availability of Privacy Policy

ACIMS provides this Privacy Policy from the Privacy link on our website at www.acimsolutions.com.au and as reasonably practical, this Privacy Policy can also be made available in a different format as requested by the individual.

4.1.11 Review and Update of this Privacy Policy

ACIMS reviews this Privacy Policy on an ongoing basis, as part of continuous improvement, or as government required changes are identified. Where this policy is updated, changes to the policy are communicated to staff and published to the ACIMS website.

4.2. OFFERING ANONYMITY OR PSEUDONYMITY

ACIMS does not require a person to identify themselves when dealing with us unless it is necessary for the individuals' information to be collected to complete a request. For example, a person can send an enquiry to ACIMS without verifying their name, however they will need to provide their legal name to enrol in a course or provide a name for billing details when purchasing items.

If there is an option to deal anonymously or by pseudonym with us, individuals will be told of this option. For example, student usernames for our learning system can be self-determined by students (either username or associated email address) so students do not need to include an individual name or identifying information.

ACIMS only stores and links pseudonyms to individual personal information in cases where this is required for service delivery (such as system login information) or once the individual's consent has been received.

4.3. COLLECTING PERSONAL INFORMATION

4.3.1 Collection of solicited personal information

ACIMS only collects personal information that is reasonably necessary for our business activities. We only collect sensitive information in cases where the individual consents to the sensitive information being collected, except in cases where we are required to collect this information by law. All information we collect is collected by lawful and fair means. We only collect solicited information directly from the individual concerned,

unless it is unreasonable or impracticable for the personal information to only be collected in this manner.

Sensitive information (such as credit card information) when collected is done so using appropriate software gateways and merchant services to ensure this information is not held or accessible to unauthorised persons.

4.3.2 Dealing with unsolicited personal information

ACIMS may occasionally receive unsolicited personal information. If it is information that we would not have collected lawfully or for a valid business purpose we will immediately destroy or de-identify the information (unless it would be unlawful to do so).

4.3.3 Notifying individuals of the collection of personal information

When ACIMS collects personal information about an individual, we take reasonable steps to notify the individual this has occurred. This includes:

- Showing ACIMS's contact details, including the position title, email address and phone number (business mobile and ACIMS business mainline) of a contact who handles enquiries and requests relating to privacy matters
- the facts and circumstances of collection such as the date, time, place and method of collection, and whether the information was collected from a third party, including the name of that party
- if the collection is required or authorised by law, including the name of the Australian law or other legal agreement requiring the collection
- the purpose of collection, including any primary and secondary purposes
- the consequences for the individual if all or some personal information is not collected
- other parties to which the information is usually disclosed, including naming those parties
- whether we are likely to disclose the personal information to overseas recipients, and if so, the names of the recipients and the countries in which such recipients are located
- a link to this Privacy Policy on our website
- advice that this Privacy Policy contains information about how the individual may access and seek correction of the personal information held by us, how to complain about a breach of the policy, and how we will deal with such a complaint

Where possible, we ensure that the individual confirms their understanding of these details, such as through signed declarations, website form acceptance of details or in person through questioning.

4.3.4 Collection from third parties

Where ACIMS collects personal information from another organisation we will confirm that relevant notice has been provided to the individual, and if this has not occurred, we will undertake this notice to ensure the individual is fully informed of the information collection.

ACIMS has enabled the Google Analytics Demographics and Interest Reporting functionality available through Google Analytics. ACIM Solutions and our associates use first-party cookies (Google Analytics cookies) and third-party cookies (the DoubleClick cookie) to collect information.

Users have the option to adjust their internet browser to reject cookies.

4.3.5 Using or disclosing personal information

ACIMS only uses or discloses personal information it holds about an individual for the particular primary purposes for which the information was collected, or secondary purposes in cases where:

- an individual consented to a secondary use or disclosure
- an individual would reasonably expect the secondary use or disclosure, and that is directly related to the primary purpose of collection, such as billing and accounts management
- using or disclosing the information is required or authorised by law.

4.3.6 Requirement to make a written note of use or disclosure for secondary purpose

If ACIMS uses or discloses personal information in accordance with an 'enforcement related activity' we will make a written note of the use or disclosure, including the following details:

- the date of the use or disclosure
- details of the personal information that was used or disclosed
- the enforcement body conducting the enforcement related activity
- if the organisation used the information, how the information was used by the organisation
- the basis for our reasonable belief that we were required to disclose the information.

4.3.7 Cross-border disclosure of personal information

We do not proactively share information overseas. ACIMS uses a third-party student management system incorporating cloud storage. This utilises Australian based storage facilities data and is protected behind high level firewalls with data being encrypted whilst stored and in transit. ACIMS has undertaken security consultations with the system provider to ensure we meet Australian Government security requirements. ACIMS takes reasonable steps to ensure that the recipient does not breach any privacy matters in relation to that information.

4.3.8 Use of personal information for direct marketing

ACIMS does not use or disclose the personal information that it holds about an individual for the purpose of direct marketing, unless:

- the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing. E.g. information to previous students of relevant courses, or provision of newsletters that a student has expressed interest in, and
- we provide a simple method for the individual to request not to receive direct marketing communications (also known as 'opting out').

4.3.9 Adoption, use or disclosure of government related identifiers

ACIMS does not adopt, use or disclose a government related identifier related to an individual except:

- in situations required by Australian law or other legal requirements
- where reasonably necessary to verify the identity of the individual
- where reasonably necessary to fulfil obligations to an agency or a State or Territory authority

- as prescribed by regulations.

4.3.10 Quality of personal information

ACIMS takes reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. We also take reasonable steps to ensure that the personal information we use or disclose is accurate, up-to-date, complete and relevant. This is important both when we initially collect the personal information, and then subsequent use or disclosure of the personal information.

Quality measures to support this include:

- internal training, practices, procedures and systems to audit, monitor, identify and correct poor quality personal information
- processes that ensure personal information is collected and recorded in a consistent format, from a primary information source when possible
- ensuring updated or new personal information is promptly added to relevant existing records
- providing individuals with a simple means to review and update their information on an on-going basis through our online portal
- reminding individuals to update their personal information at critical service delivery points
- contacting individuals to verify the quality of personal information where appropriate when it is about to be used or disclosed, particularly if there has been a lengthy period since collection
- checking that any third party, from whom personal information is collected, has implemented appropriate data quality practices, procedures and systems.

4.4. ENSURING SECURITY AND ACCURACY OF PERSONAL INFORMATION

ACIMS takes active measures to ensure we are correct to retain personal information we hold, and also to ensure the security of personal information we hold. This includes reasonable steps to protect the information from misuse, interference and loss, unauthorised access, modification or disclosure.

We destroy or de-identify personal information held once the information is no longer needed for any purpose for which the information may be legally used or disclosed.

Staff and sub-contractors are provided with training regarding privacy and records management as part of their induction with ACIMS, as appropriate to their role and access to information. Information about updates to privacy requirements and reminders about requirements are provided to personnel as needed.

Staff, sub-contractors and students are encouraged to take reasonable steps to protect their information that we hold by keeping their passwords secret and ensuring they log out systems when a task is complete.

Personal data is not placed through AI platforms and tools where this data could be exposed. AI tools built into systems, such as the Student Management System and Learning Management System, may be used by ACIMS to assist with analytics about RTO performance and student requirements. AI systems are reviewed, tested and evaluated prior to use and consideration given to the impacts on stakeholders of information involved in the system use.

ACIMS is not responsible for the privacy or security of third-party websites that individuals access via links on the ACIM Solutions website.

5. PROCEDURES

5.1 GAINING ACCESS TO PERSONAL INFORMATION

Before giving access to personal information, ACIMS will confirm the identity of the individual making the request, to ensure it is the individual or a person who is authorised to make a request on their behalf.

The minimum amount of personal information needed to establish an individual's identity is to be sought, which is generally:

- an individual's name
- date of birth
- last known address
- service details.

This applies when meeting the requesting party in person or over a telephone/video conference.

ACIMS will then confirm what information is required to be accessed and the format in which the information sought is required. Where the requested format is not practical, ACIMS will consult with the requester to ensure a format is provided that meets the requester's needs.

The next step is for ACIMS to respond to the request for access to information. The decision will be to complete the request or refuse the request:

Completion of request	Refusal of request
<p>ACIMS will search records that we possess or control to assess whether the requested personal information is contained in those records.</p> <p>Any personal information found is to be collated ready for access.</p> <p>The access to the information is to be provided in the format in which it was requested.</p> <p>A request needs to be completed within 14 calendar days.</p> <p>The access to the requested information is to be provided free of charge.</p>	<p>A request may be refused if:</p> <ul style="list-style-type: none">• The identity or authorisation access cannot be confirmed• There is another valid reason why ACIMS is unable to provide the personal information <p>Refusal to provide access to records will be provided to the requester in writing.</p> <p>The notification will include reason(s) for the refusal, and the complaint mechanisms available to the individual.</p> <p>The notifications is to be provided within 14 calendar days of receipt of the original request.</p> <p>There is to be no charge for this.</p>

5.2 CORRECTING OR UPDATING PERSONAL INFORMATION

Before correcting or updating personal information, as above, ACIMS will identify the individual concerned and confirm their identity of the individual or party to whom the record relates.

ACIMS will then search the records that we possess or control to confirm if the pertinent personal information is contained in those records and assess the information to determine whether the requested update should proceed. This may include checking

information against other records held by us or within government databases that we access, in order to complete an assessment of the correct version of the information to be used.

ACIMS will then decide to correct/update the information as per the request or decline this update request:

Completion of request	Refusal of request
<p>The identified personal information contained in the records is to be corrected or updated.</p> <p>The update will be notified to any relevant third parties of corrections made to personal information, if this information was previously provided to these parties.</p> <p>The update is to be completed within 14 calendar days.</p> <p>The update is to be provided free of charge.</p>	<p>A request may be refused if:</p> <ul style="list-style-type: none"> • If the identity or authorisation access cannot be confirmed • There is another valid reason why ACIMS is unable or unwilling to update the personal information <p>Refusal to update the information will be provided to the requester in writing.</p> <p>The notification will include reason(s) for the refusal, and the complaint mechanisms available to the individual.</p> <p>The notifications is to be provided within 14 calendar days of receipt of the original request. There is to be no charge for this.</p> <p>If requested by the individual, reasonable steps will be taken by ACIMS to associate a statement with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading.</p>

5.3 MAKING A PRIVACY COMPLAINT

If an individual feels that ACIMS has breached its obligations in the handling, use or disclosure of their personal information, they may raise a complaint. We encourage individuals to discuss the situation with the ACIMS General Manager in the first instance, before making a formal complaint.

The complaints handling process is as follows:

The individual should make the complaint including details about the issue in writing to:

ACIM Solutions CEO
 c/o contact@acimsolutions.com.au or PO Box 3190 Valentine NSW 2280
 Phone: 1300 224 677

ACIMS will investigate the circumstances included in the complaint and respond to the individual as soon as possible (within 30 calendar days) regarding its findings and actions following this investigation.

If after considering this response the individual is still not satisfied, they make escalate their complaint directly to the Information Commissioner for investigation:

Office of the Australian Information Commissioner
www.oaic.gov.au
 Phone: 1300 363 992

6. RESPONSIBILITIES

Ensuring compliance with the Privacy Policy is the responsibility of all ACIM Solutions staff and sub-contractors.

The ACIM Solutions CEO retains accountability for the compliance of the organisation with legislative requirements.

It is the responsibility of students and other third parties such as employers to provide accurate and up to date personal information to ACIM Solutions in line with this Privacy Policy.

7. MONITORING AND EVALUATION

The Compliance Officer will monitor changes to Privacy Legislation requirements and recommend updates to the policy as required.

The policy is to be reviewed annually to ensure currency with requirements, and to be updated as changes to relevant legislation or ACIM Solutions procedures occur.

The policy must also be reviewed and evaluated following any complaints relating to privacy.

8. DOCUMENTATION

Document control	
Version and Creation Date	Version 2.2 November 2025
Review Due Date	<ul style="list-style-type: none">• November 2026 – to ensure currency – with any redesign as required• As updates occur to relevant legislation
Creation Contact	Kathryn Burke - Compliance Officer
Final Approval	Philippa Woolf - Owner/CEO