CPR FIRST AID

P006

PRIVACY POLICY AND PROCEDURE

RTO 21903 | ABN 75 134 879 315

Version	2.0 - Draft for approval
Prepared	13 July 2026
Effective date	13 July 2026
Supersedes	Version 1.1, revised 16 April 2019

Document status

This document is a compliance-ready draft. It must be approved, published and implemented through CPR First Aid's enrolment, website, marketing, records, vendor and incident-management processes before it is represented as the organisation's operative policy.

Public policy and internal operating procedure

Document control

Policy number	P006
Policy owner	Privacy Officer / Compliance Manager
Accountable officer	Chief Executive Officer or authorised governing person
Approval date	To be completed on approval
Review cycle	At least annually, and earlier when law, standards, systems, vendors, data practices or incidents change
Next scheduled review	Within 12 months after approval
Applies to	Students, prospective students, clients, staff, trainers, assessors, contractors, training partners, suppliers and website users
Availability	Published free of charge on the CPR First Aid website and available in an accessible format on request

Version history

Version	Date	Status	Summary	Author/owner
1.1	16 Apr 2019	Superseded	Previous policy and procedure.	RTO Excellence
2.0	13 Jul 2026	Draft	Full revision for current privacy, ASQA, VET data, USI, security and breach requirements.	Privacy Officer

Related controlled documents and records

- Student Handbook and enrolment terms
- Current VET privacy notice used at or before enrolment
- Enrolment form and student declaration
- Complaints and appeals policy and register
- Records management and retention schedule
- Information security and acceptable-use controls
- Data breach response plan and data breach register
- Marketing consent and suppression records
- Vendor, cloud service and overseas disclosure register
- Staff induction, confidentiality and privacy training records

Controlled external wording

The minimum VET privacy notice is not reproduced as static text in this policy. CPR First Aid must use the current government-approved notice that applies to its reporting pathway: the National VET Data Policy notice while reporting under AVETMISS, or the approved VET Information Standard enrolment notice after transition.

Contents

PART A - PRIVACY POLICY

1. Purpose

This policy explains how CPR First Aid collects, holds, uses, discloses, protects, provides access to, corrects, retains and disposes of personal information. It is intended to support compliance with Australian privacy law, the requirements applying to an ASQA-regulated registered training organisation, VET data obligations and the Unique Student Identifier framework.

The objectives are to protect individuals, preserve the integrity and availability of training records, ensure that CPR First Aid can demonstrate accountable privacy practices, and provide practical instructions for staff, trainers, contractors and service providers.

2. Scope

This policy applies to:

- All personal information and sensitive information held or controlled by CPR First Aid, whether in electronic, paper, audio, video, photographic or other form;
- All business units, locations, websites, online portals, learning systems, student management systems, payment systems, email, shared drives, portable devices and archives;
- All directors, governing persons, employees, trainers, assessors, contractors, consultants, volunteers, training partners and authorised service providers; and
- Information about prospective, current and former students, clients, employer contacts, website users, complainants, staff, applicants and other individuals.

Where an employee-record exemption or another statutory exception applies, CPR First Aid will still handle the information in accordance with this policy as far as practicable and will comply with all other applicable workplace, tax, superannuation, health-records and confidentiality obligations.

3. Policy commitments

CPR First Aid will:

- Collect only information that is reasonably necessary for legitimate functions and activities, and collect sensitive information only with consent or another lawful basis;
- Give clear privacy notices at or before collection, including the current VET privacy notice at or before enrolment;
- Use and disclose information only for the purpose notified, a related lawful purpose, with consent, or as required or authorised by law;
- Take reasonable technical and organisational measures to protect information throughout its lifecycle;
- Enable individuals to access and correct their information, subject to lawful exceptions;
- Respond fairly and promptly to privacy complaints and suspected data breaches;
- Retain records only for an approved legal, regulatory, contractual or operational period and then securely destroy or de-identify them; and
- Review privacy risks when introducing or changing systems, vendors, data uses, analytics, artificial intelligence or automated decision-making.

4. Definitions

Term	Meaning
APPs	The Australian Privacy Principles in Schedule 1 to the Privacy Act 1988 (Cth).
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.
Sensitive information	A category of personal information that includes health information, disability or support information, racial or ethnic origin, Aboriginal or Torres Strait Islander status, criminal record, biometric information and other categories defined by the Privacy Act.
Data breach	Loss, unauthorised access, unauthorised disclosure, or another compromise of personal information.
Eligible data breach	A data breach that is likely to result in serious harm to one or more individuals and for which remedial action has not prevented the likely serious harm, subject to the Privacy Act.
USI	Unique Student Identifier created and managed under the Student Identifiers Act 2014.
VET data	Information about VET students, training activity, providers, courses and outcomes collected and reported under national VET requirements.
Hold	To possess or control a record containing personal information, including information held by a service provider where CPR First Aid retains control.
Privacy Officer	The role appointed by CPR First Aid to oversee privacy compliance, requests, complaints, incidents, registers and reviews.

5. Legislative and regulatory framework

CPR First Aid will apply this policy consistently with the current versions of applicable requirements, including:

- Privacy Act 1988 (Cth), the Australian Privacy Principles and the Notifiable Data Breaches scheme;
- National Vocational Education and Training Regulator Act 2011 (Cth);
- 2025 Standards for Registered Training Organisations, including the applicable Outcome Standards and Compliance Standards;
- National Vocational Education and Training Regulator (Data Provision Requirements) Instrument 2020, as amended, including the 2026 Data Streamlining amendments;
- National VET Data Policy while CPR First Aid reports under AVETMISS, and the VET Information Standard and associated requirements after transition;
- Student Identifiers Act 2014 and applicable regulations, exemptions, terms and conditions;
- Spam Act 2003 and applicable telemarketing requirements;
- Applicable Commonwealth, State and Territory tax, employment, health-records, funding, licensing, recordkeeping and contractual requirements; and
- Lawful notices, directions, court or tribunal orders and regulator requirements.

Where requirements conflict, the Privacy Officer will obtain appropriate legal or regulator guidance and document the basis for the adopted approach.

6. Roles and responsibilities

Role	Responsibilities
Governing persons / CEO	Approve this policy, provide resources, oversee material privacy risks and receive reports on serious incidents and systemic non-compliance.
Privacy Officer / Compliance Manager	Maintain the policy, registers and notices; advise staff; manage access, correction, complaints and breaches; review vendors and overseas disclosures; monitor implementation; and report to governance.
Managers	Implement controls in their areas, minimise collection, approve access, ensure staff training and escalate privacy risks or incidents.
Staff, trainers and contractors	Follow this policy, use only authorised systems, protect credentials and devices, collect only necessary information and immediately report suspected incidents.
ICT and system administrators	Apply access controls, logging, backups, patching, secure configuration, account lifecycle controls and incident support.
Marketing personnel and providers	Maintain consent evidence, honour opt-outs, use approved lists and templates, and comply with privacy and spam requirements.
Vendors and training partners	Comply with contractual privacy, security, confidentiality, deletion, incident notification and audit requirements.

7. Open and transparent privacy management

CPR First Aid will maintain practices, procedures and systems that support compliance with this policy and the APPs. The public-facing privacy policy will be available free of charge on the website and in an accessible format on request.

The Privacy Officer will maintain, at minimum:

- A personal-information asset and system register;
- A vendor, cloud service, data-location and overseas disclosure register;
- A retention and disposal schedule;
- Privacy complaint, access, correction and data breach registers;
- Evidence of current enrolment and point-of-collection notices;
- Records of privacy impact assessments for material changes;
- Staff training, confidentiality and access-approval records; and
- An annual privacy compliance review and remediation plan.

8. Collection, anonymity and notification

8.1 Information CPR First Aid may collect

- Identity and contact information, including legal name, date of birth, address, email and telephone number;
- Enrolment, attendance, assessment, competency, certification and course-progress information;
- USI and information needed to verify or create a USI where authorised;
- VET statistical information, including demographic, language, disability, schooling, employment and Indigenous-status information required or permitted by the applicable data standard;
- Support, accessibility, health or safety information reasonably needed to provide training safely and fairly;
- Payment, invoicing, employer booking and transaction information;
- Communications, complaints, feedback, survey responses and call or session records where notified;
- Website, device, log, cookie and analytics information;

- Staff, contractor, trainer and applicant information, including qualifications, currency, employment, tax, superannuation and screening records; and
- Other information required by law, a funding arrangement, licensing body or legitimate business function.

8.2 Collection rules

Personal information will be collected by lawful and fair means and, where reasonable and practicable, directly from the individual. CPR First Aid will:

- Test whether each field or document is reasonably necessary before collecting it;
- Avoid collecting full identity documents where sighting or verification is sufficient;
- Obtain consent before collecting sensitive information unless an exception applies;
- Use secure collection channels and restrict free-text fields that may invite unnecessary sensitive information;
- Record the source and authority where information is collected from an employer, guardian, job service provider, government body, training partner or other third party; and
- Provide or refer to an APP 5 collection notice at or before collection, or as soon as practicable afterwards where permitted.

8.3 Anonymity and Pseudonymity

Individuals may deal with CPR First Aid anonymously or by pseudonym where lawful and practicable, including for general enquiries or anonymous feedback. Identification is required where CPR First Aid must verify identity, enrol a student, report VET activity, issue AQF certification, process a payment, manage safety, investigate a matter fairly, or meet another legal obligation.

8.4 Unsolicited information

Where unsolicited personal information is received, the recipient must promptly determine whether CPR First Aid could lawfully have collected it. If not, and retention is not required by law, the information must be securely destroyed or de-identified. Unnecessary copies and attachments must not be retained merely because they were received.

9. VET data and Unique Student Identifier handling

9.1 VET privacy notice

At or before enrolment, CPR First Aid must provide the current minimum privacy notice applicable to its reporting pathway. The enrolment process must capture evidence that the notice was displayed or provided. The notice must explain why information is collected, how it is used and shared, and how the student can seek access, correction or make a complaint.

Transition rule

Until CPR First Aid formally transitions to the VET Information Standard, it may continue reporting under AVETMISS where permitted and must use the current National VET Data Policy notice. After transition, it must use the approved VET Information Standard enrolment notice and meet the associated data responsibilities.

9.2 VET data reporting

CPR First Aid will collect, validate, correct and report VET data to NCVER, government departments, regulators, State or Territory Training Authorities and other authorised bodies as required. Data must be accurate, complete, timely and limited to the authorised purpose. Reporting files and correction activity must be protected and auditable.

9.3 USI

CPR First Aid will:

- Collect, verify, use and disclose a USI only as permitted by the Student Identifiers framework;
- Obtain the required authorisation before searching for or creating a USI on behalf of an individual;
- Not ask for or store a student's USI account password, security answers or multi-factor authentication credentials;
- Not activate another person's USI account or take control of that account;
- Limit access to USIs to authorised personnel and authorised systems;
- Not print or display the USI on AQF certification documentation;
- Obtain permission before viewing or sharing a student's VET transcript where permission is required; and
- Destroy copies of identity documents collected solely for a USI transaction as soon as the transaction is complete and the documents are no longer required.

10. Use and disclosure

CPR First Aid will use or disclose personal information for the primary purpose for which it was collected, for a related secondary purpose that the individual would reasonably expect, with consent, or where required or authorised by law.

Depending on the circumstances, authorised recipients may include:

- ASQA, NCVER, DEWR, State or Territory Training Authorities and other authorised government agencies;
- The Student Identifiers Registrar and USI Registry System;
- Employers, schools, guardians, job service providers or booking organisations where the individual has authorised the disclosure or another lawful basis applies;
- Trainers, assessors, auditors, consultants, insurers, lawyers, payment providers and technology service providers who need the information to perform authorised functions;
- Emergency services, health or safety personnel where necessary to prevent or lessen a serious threat or address an emergency;
- Courts, tribunals, enforcement bodies and regulators where required or authorised; and
- Another RTO or authorised entity where the student has consented or a transfer, teach-out or closure arrangement lawfully requires it.

Only the minimum information reasonably necessary for the disclosure will be provided. Material or unusual disclosures must be recorded, including the recipient, date, information disclosed, authority and approving officer.

11. Direct marketing

CPR First Aid may send information about training and related services where consent exists or the communication is otherwise permitted. Marketing lists must be separated from mandatory student communications.

Commercial electronic messages must:

- Be supported by express or inferred consent that CPR First Aid can evidence;
- Accurately identify the sender and include current contact details;
- Contain a clear, functional and low-cost unsubscribe facility;
- Not require an individual to log in, create an account or provide additional personal information to unsubscribe; and
- Have unsubscribe requests actioned within five working days, with suppression records maintained to prevent re-contact.

Personal information will not be sold. A contracted marketing provider may process information only under a written agreement and CPR First Aid remains responsible for oversight.

12. Overseas recipients and cloud services

CPR First Aid may use cloud, communications, analytics, payment, support or other providers that store or access information outside Australia. Before a new or changed arrangement is approved, the Privacy Officer must assess data location, remote access, sub-processors, security, contractual protections, breach notification, deletion and APP 8 accountability.

Where personal information is likely to be disclosed to overseas recipients, CPR First Aid will take reasonable steps required by APP 8, identify likely countries in the public privacy policy or collection notice where practicable, and maintain the vendor and overseas disclosure register. CPR First Aid will not state that all records are stored in Australia unless this has been verified for every relevant system, backup, support and sub-processor.

13. Government-related identifiers

Government-related identifiers, including a USI, tax file number, driver licence number, passport number, Medicare number or concession number, will not be adopted as CPR First Aid's own identifier. They will be collected, used, disclosed and stored only where reasonably necessary and permitted by law.

Full identifier numbers must not be copied into notes, email subject lines, filenames or uncontrolled spreadsheets. Access must be restricted, and masking should be used where the complete number is not required.

14. Data quality

CPR First Aid will take reasonable steps to ensure personal information is accurate, up to date, complete, relevant and not misleading, having regard to the purpose for which it is used or disclosed.

- Students will be invited to verify key details at enrolment and before certification.
- USIs and names will be validated using authorised processes.
- Material corrections will be propagated to relevant systems and authorised recipients where required.
- Duplicate records will be investigated and merged only through an approved, auditable process.
- VET data validation errors will be corrected and resubmitted within applicable timeframes.

15. Security of personal information

CPR First Aid will take reasonable technical and organisational measures proportionate to the nature, volume, sensitivity and consequences of compromise of the information it holds.

15.1 Organisational measures

- Privacy and security responsibilities assigned to accountable roles;
- Privacy-by-design and risk assessment for material changes;
- Staff induction, annual refresher training and confidentiality obligations;
- Least-privilege access approval, periodic access reviews and prompt removal of access when no longer required;
- Documented incident, continuity, backup, recovery, retention and disposal processes;
- Vendor due diligence and written privacy and security clauses; and
- Monitoring, audit, corrective action and governance reporting.

15.2 Technical and Physical measures

- Unique user accounts and multi-factor authentication for systems where available and appropriate;
- Strong authentication, password management and prohibition on credential sharing;
- Encryption in transit and, where available and proportionate, encryption at rest;
- Secure configuration, patching, anti-malware, logging and monitoring;
- Device encryption, automatic screen locking and secure remote access;
- Regular backups and recovery testing;
- Role-based permissions in student, learning, finance and document systems;
- Secure file transfer rather than uncontrolled email attachments where feasible;
- Locked storage for paper records and controlled access to archives;
- Secure shredding, certified destruction or verified electronic deletion; and
- Restrictions on personal devices, personal email, removable media and local copies.

15.3 Trainer and mobile-work controls

Trainers and assessors must not retain student lists, assessment evidence, identity documents or health/support information on personal devices or in personal cloud accounts. Any authorised temporary local copy must be encrypted, used only for the approved purpose, uploaded to the authorised system promptly and securely deleted.

16. Access and correction

16.1 Access

- An individual may request access to personal information CPR First Aid holds about them. Requests may be made by any reasonable channel and do not need special wording. CPR First Aid will verify identity proportionately, without collecting unnecessary identifiers.
- The request will be acknowledged as soon as practicable, normally within five business days.
- A response will ordinarily be provided within 30 calendar days.
- No fee is charged for making a request. A reasonable, non-excessive charge may be imposed for giving access only where lawful and advised in advance.
- Access will be provided in the requested manner where reasonable and practicable.
- Where an APP 12 exception applies, CPR First Aid will consider whether partial access, redaction, an intermediary or another form of access is possible.
- A refusal or limitation will be explained in writing, including available complaint mechanisms, unless the law permits reasons to be withheld.

16.2 Correction

An individual may ask CPR First Aid to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading. CPR First Aid may also correct information on its own initiative.

- Correction requests will ordinarily be completed within 30 calendar days.
- No charge will be imposed for making or actioning a correction request.
- Where appropriate and lawful, relevant third parties previously given the information will be notified of the correction.
- If a correction is refused, CPR First Aid will provide written reasons and, on request, associate a statement with the record that the individual considers it inaccurate or otherwise deficient.

17. Privacy complaints

A person may complain about how CPR First Aid has handled personal information or complied with this policy. Complaints may be made by email, telephone, post or another accessible channel.

- The complaint will be recorded and acknowledged, normally within five business days.
- The investigator will be sufficiently independent from the subject of the complaint.
- The complainant will be given a fair opportunity to provide relevant information.
- CPR First Aid will aim to provide a written outcome within 30 calendar days. If more time is reasonably needed, the complainant will be told why and given a revised date.
- Outcomes may include correction, access, deletion where lawful, apology, process change, training, vendor action or another proportionate remedy.
- If the complainant is not satisfied, they may complain to the Office of the Australian Information Commissioner or another applicable external body.

18. Data breach management

All suspected privacy incidents must be reported immediately to the Privacy Officer or designated incident contact. Staff must not delay reporting while attempting to investigate or fix the matter themselves.

CPR First Aid will:

- Contain the incident, protect affected systems and preserve relevant evidence;
- Identify the information, individuals, systems, recipients and third parties involved;
- Assess the risk of harm, including identity fraud, financial harm, physical or psychological harm, discrimination, reputational harm and loss of control over sensitive information;
- Complete an eligible data breach assessment as quickly as practicable and, wherever possible, within 30 days;
- Take remedial action to reduce or prevent serious harm;
- Notify the OAIC and affected individuals as soon as practicable where an eligible data breach has occurred, unless an exception applies;
- Coordinate notifications where more than one entity is involved;
- Record decisions, evidence, advice, notifications and remedial actions; and
- Conduct a post-incident review and implement corrective actions.

19. Retention, destruction and de-identification

Personal information will be retained only for the approved period needed to satisfy legal, regulatory, funding, contractual, dispute, safety and legitimate operational requirements. Retention periods apply to all copies, including email, shared drives, local files, archives and backups to the extent reasonably practicable.

AQF certification documentation records must be retained for 30 years. Assessment submissions for students completing a training product on or after 1 July 2025 must be retained for two years after completion, unless a longer period applies under a licensing, funding, contractual or other legal requirement.

When information is no longer required, CPR First Aid will take reasonable steps to securely destroy it or ensure it is effectively de-identified. Destruction must be suspended where a legal hold, complaint, investigation, audit or anticipated dispute requires preservation.

20. Websites, cookies, payments, recordings and online learning

20.1 Website and analytics

The website may collect technical information such as IP address, browser, device, page activity, referring source and cookie identifiers. Collection notices and cookie controls must accurately describe the technologies used, their purposes, relevant providers, choices and any overseas processing.

CPR First Aid will not guarantee that online transactions or systems are '100% secure'. Public statements will accurately describe the reasonable safeguards in place and acknowledge that no method of electronic transmission or storage is completely risk-free.

20.2 Payments

Payment-card information should be processed through an authorised payment provider and should not be stored in CPR First Aid systems unless specifically approved and protected. Staff must not request card details through ordinary email or write them in free-text notes.

20.3 Calls, photographs, video and online sessions

Where calls, classes, online sessions, assessments, photographs or video are recorded, participants must be notified before recording unless an exception applies. The notice must explain the purpose, access, retention and available alternatives where practicable. Recordings must not be reused for marketing, training or analytics without an appropriate lawful basis.

21. Children, representatives, employers and third-party bookings

Where a student is under 18 or another person acts through a representative, CPR First Aid will assess the student's capacity, the representative's authority and the purpose of the request. A parent, guardian, employer or booking contact does not automatically have unrestricted access to a student's assessment, support, complaint or health information.

Only necessary information will be disclosed to employers, schools, guardians or booking organisations under consent, contract or another lawful authority. Sensitive support or health information will be shared on a need-to-know basis.

22. Staff and contractor information

CPR First Aid may collect information needed for recruitment, engagement, payroll, superannuation, performance, qualifications, trainer currency, safety, conduct, screening, insurance and legal compliance. Access will be restricted to authorised personnel.

Unsuccessful applicant records and expired staff documents will be disposed of according to the retention schedule unless consent or a legal requirement supports longer retention. Tax file numbers and other high-risk identifiers require enhanced controls.

23. Automated decisions

Before implementing a computer program that makes, or substantially assists in making, decisions that could reasonably be expected to significantly affect an individual's rights or interests, CPR First Aid will complete a privacy impact assessment, test data quality and bias risks, establish human oversight and review rights, and update its public privacy policy and collection notices.

Review trigger - 10 December 2026

Additional APP 1 privacy-policy transparency requirements for certain substantially automated decisions commence on 10 December 2026. This policy should be checked again before that date and whenever CPR First Aid introduces material AI or automated decision tools.

24. Monitoring and review

The Privacy Officer will review this policy at least annually and earlier following significant legal or regulatory change, a material incident, new system or vendor, new collection practice, transition to the VET Information Standard, material complaint trend, audit finding or change to business operations.

Monitoring will include:

- Sampling enrolments to confirm the correct privacy notice was provided;
- Reviewing access permissions, inactive accounts and trainer-device practices;
- Testing unsubscribe and suppression processes;
- Reviewing deletion and retention evidence;
- Checking vendor assurance and data-location information;
- Reviewing complaints, incidents and data-quality corrections for trends; and
- Reporting material findings, overdue actions and residual risks to governance.

PART B - OPERATING PROCEDURES

Procedure 1 - Collection and privacy notices

1. Identify the business purpose, legal authority, recipients, system, retention period and whether sensitive information is involved.
2. Apply data minimisation: remove fields, documents or free-text collection that are not reasonably necessary.
3. Select or prepare the correct collection notice. For students, include the current VET notice applicable to CPR First Aid's reporting pathway.
4. Provide the notice at or before collection and configure the system to retain evidence that the notice was displayed or supplied.
5. Obtain and record consent where required, particularly for sensitive information, optional marketing, recordings or secondary uses.
6. Use an approved secure channel and restrict access to authorised roles.
7. Record the information asset, system, vendor, retention and overseas-processing details in the relevant registers.
8. Reassess the notice and purpose whenever the form, system, recipient, vendor or use changes.

Procedure 2 - VET data and USI

2.1 Enrolment and VET data

9. Confirm whether CPR First Aid is reporting under AVETMISS or has formally transitioned to the VET Information Standard.
10. Use the current approved enrollment privacy notice and student declaration for that reporting pathway.
11. Validate mandatory fields and explain the consequences of not providing information where relevant.
12. Restrict VET reporting exports to authorised personnel and secure transmission channels.
13. Review validation errors, correct source records and resubmit data as required.
14. Retain evidence of notices, declarations, submissions, corrections and authority for disclosures.

2.2 USI transaction

15. Ask the student to provide and, where required, verify their USI through an authorised system.
16. Where CPR First Aid searches for or creates a USI, obtains and retains the required authorisation and consent evidence.
17. Sight or securely receive the minimum identity evidence required. Do not record passwords, security answers or MFA codes.
18. Complete the transaction through the authorised USI service.
19. Record the outcome and any permitted reference needed for audit.
20. Securely destroy identity-document copies collected solely for the USI transaction when no longer required.
21. Confirm that the USI is not printed on certification documentation.

Procedure 3 - Access and correction requests

22. Receive the request through any reasonable channel and forward it promptly to the Privacy Officer.
23. Open an entry in the access/correction register and acknowledge the request, normally within five business days.
24. Verify identity proportionately. Use existing account or enrolment information where possible and do not automatically require a USI or full identity-document copy.
25. Clarify scope where necessary without creating unnecessary barriers.
26. Search all relevant systems, email, archives and service providers under CPR First Aid's control.
27. Review lawful exceptions and the privacy of other individuals. Consider redaction, partial access or an intermediary.

28. Provide access or correction, ordinarily within 30 calendar days, in a secure and usable form.
29. Where refusing or limiting the request, provide written reasons and complaint options unless reasons may lawfully be withheld.
30. Propagate approved corrections to relevant systems and recipients and close the register entry with evidence.

Procedure 4 - Privacy complaints

31. Record the complaint and acknowledge it, normally within five business days.
32. Assess immediate risks and determine whether the complaint also indicates a data breach, safety issue, discrimination concern or regulatory-reporting obligation.
33. Assign an impartial investigator and define the issues, evidence and requested outcome.
34. Give the complainant a reasonable opportunity to provide information and respond to material adverse matters where appropriate.
35. Analyse compliance with the law, this policy, notices, consent, contracts and actual system records.
36. Provide a written outcome within 30 calendar days where practicable, including findings, reasons, remedial action and external escalation options.
37. Implement and verify corrective actions and record systemic improvements.
38. Retain the complaint file under restricted access and report material trends to governance.

Procedure 5 - Data breach response

1. Report and escalate

- Immediately notify the Privacy Officer or incident contact.
- Record the time detected, reporter, systems, information and known actions.
- Do not delete evidence, contact external parties or make public statements without authority.

2. Contain

- Stop or limit the unauthorised access or disclosure where safe.
- Reset credentials, revoke links, recover documents, isolate devices or suspend integrations as appropriate.
- Engage ICT, vendors, insurers, legal advisers or law enforcement where authorised.

3. Investigate

- Identify what happened, when, affected information and individuals, recipients, security controls and likely further disclosure.
- Preserve logs, emails, screenshots, audit trails and communications.
- Assess sensitivity, encryption, ease of identification and possible harms.

4. Evaluate NDB obligations

- Determine whether unauthorised access/disclosure or loss is likely to cause serious harm.
- Consider whether effective remedial action has removed the likelihood of serious harm.
- Complete the assessment as quickly as practicable and, wherever possible, within 30 days.
- Document the decision and evidence, including where notification is not required.

5. Notify and support

- Where an eligible data breach exists, prepare the required statement and notify the OAIC and affected individuals as soon as practicable.
- Give practical protective steps, a contact point and accessible support information.
- Coordinate with other affected entities so notification is accurate and not duplicated.

6. Recover and improve

- Restore services securely, monitor for recurrence and confirm corrective actions.
- Conduct a post-incident review covering root cause, control gaps, vendor issues, training, retention and notification effectiveness.
- Report material incidents and overdue actions to governance.

Procedure 6 - Retention and secure disposal

39. Classify the record using Appendix 1 and identify any longer legal, licensing, funding, contractual or legal-hold requirement.
40. Configure system retention, archiving and deletion settings where possible.
41. At least annually, identify records that have reached the end of the approved period.
42. Confirm that no complaint, investigation, audit, litigation or other hold requires preservation.
43. Destroy paper using secure shredding or an approved destruction provider.
44. Delete electronic records from active systems, local devices, email and accessible archives; address backups when reasonably practicable under the backup lifecycle.
45. Obtain and retain deletion or destruction evidence for high-risk or bulk records.
46. Update the disposal register and investigate deletion failures.

Procedure 7 - Vendors and overseas disclosures

47. Identify the information, purpose, user groups, integrations, countries, support access and sub-processors.
48. Assess privacy, security, breach history, certifications, encryption, authentication, access controls, backups, retention, deletion and business continuity.
49. Determine whether the arrangement involves an overseas disclosure and what APP 8 steps are required.
50. Use written terms covering permitted use, confidentiality, security, sub-processors, audit, breach notification, assistance with access/correction, return/deletion and exit.
51. Obtain approval from the Privacy Officer and accountable manager before production use.
52. Record the vendor, systems, countries and review date in the register and update public notices where required.
53. Review material vendors periodically and on significant change, incident or contract renewal.
54. At termination, revoke access, export required records and obtain deletion confirmation.

Procedure 8 - Direct marketing

55. Confirm the legal basis and retain evidence of express or inferred consent.
56. Keep operational communications separate from optional marketing.
57. Use only approved templates and authorised marketing systems.
58. Check the suppression list before each campaign.
59. Include clear sender identification and an unsubscribe facility that remains functional for the required period.
60. Action unsubscribe requests within five working days and retain only the minimum suppression record needed to prevent future contact.
61. Audit outsourced providers and investigate complaints, bounces, list sources and unexpected re-subscriptions.

Appendix 1 - Minimum retention schedule

The periods below are default minimum or maximum operating rules and must be read with applicable legal, funding, licensing and contractual requirements. Where a longer requirement applies, document it in the retention register. Where no requirement remains, do not retain information merely because storage is available.

Record class	Default period / trigger	Notes
AQF certification documentation and issuance register	30 years from issue	2025 Compliance Standards / AQF requirements
Student assessment submissions	2 years after completion of the training product	Longer if required by licensing, funding, contract or law
Enrolment, attendance, outcome, declaration and core student administration records	7 years after final activity, except information incorporated into the 30-year certification record	Review for data minimisation and any specific funding requirement
VET data submissions, validation and correction evidence	7 years after the relevant reporting period, or longer if required	Protect as restricted student data
USI value and verification record	For the period necessary to deliver, report and evidence training obligations	USI must not appear on certification documentation
Identity-document copies collected only for a USI transaction	Destroy promptly when the transaction is complete and no longer required	Do not retain as a convenience copy
Payment and accounting records	At least 5 years, or the longer period required by tax/corporations law	Do not retain full payment-card details unless specifically approved
Access, correction and privacy complaint files	7 years after closure	Restrict access; retain evidence of response and remedy
Data breach and security incident records	7 years after closure, or longer for material incidents	Include assessment, notification and corrective actions
Marketing consent evidence	While relied upon and for 5 years after last relevant communication	Evidence must identify source, date and scope
Marketing suppression / unsubscribe record	As long as reasonably necessary to honour the opt-out	Retain only minimum contact identifier and suppression status
Staff payroll and employment records	7 years after employment ends, or the applicable statutory period	Some records may require different periods
Unsuccessful recruitment records	Normally 12 months after recruitment closes	Longer only with consent, legal hold or documented need
Vendor due-diligence, contract and deletion evidence	7 years after contract ends	Longer where linked to an incident or dispute
Website, system and security logs	Shortest period reasonably required; normally no more than 24 months unless needed for security, audit or law	Document per system in the information asset register

Appendix 2 - Required registers and evidence

Register / evidence	Minimum content
Privacy compliance register	Review dates, findings, corrective actions, owners and closure evidence.
Personal-information asset register	Data categories, purposes, systems, owners, access, sensitivity, recipients, retention and disposal method.
Vendor and overseas disclosure register	Provider, service, data, countries, sub-processors, contract, due diligence, review and exit status.
Privacy notice register	Form or channel, notice version, reporting pathway, publication date and evidence of display.
Access and correction register	Request date, identity verification, scope, searches, decision, response date and outcome.
Privacy complaint register	Issues, investigator, evidence, findings, response, remedy and systemic action.
Data breach register	Detection, containment, investigation, harm assessment, NDB decision, notifications, recovery and lessons.
Retention and disposal register	Record class, authority, due date, hold status, disposal method, evidence and approver.
Marketing consent and suppression records	Consent source, wording, date, scope, campaigns, opt-out date and suppression status.
Training and confidentiality records	Induction, refresher training, attestations, contractor terms and follow-up.

Appendix 3 - Approval and implementation checklist

Complete before publication

The policy is not fully implemented until the following items have been confirmed and evidence retained.

- ☐ Confirm and record the approving officer, approval date, effective date and next review date.
- ☐ Confirm the current Privacy Officer role, monitored email address and telephone contact.
- ☐ Confirm CPR First Aid's current postal/head-office address and correct any inconsistent postcode or legacy address across documents.
- ☐ Confirm whether CPR First Aid currently reports under AVETMISS or has formally transitioned to the VET Information Standard.
- ☐ Replace the enrolment notice and declaration with the current government-approved wording for the applicable reporting pathway.
- ☐ Update the public website privacy policy and remove legacy references to National Privacy Principles, 2012 standards, obsolete clauses, and '100% secure' claims.
- ☐ Inventory all systems and vendors, including the student management system, LMS, website, analytics, email, payments, communications, backups and support providers.
- ☐ Identify data storage and support-access countries and update the public privacy policy with likely overseas countries where practicable.

- [ ] Confirm the retention schedule against funding contracts, State/Territory requirements, licensing rules and actual system settings.
- [ ] Implement or confirm the data breach response contacts, register, escalation path and notification authority.
- [ ] Implement access reviews, MFA, device controls, trainer handling rules, secure deletion and vendor exit evidence.
- [ ] Test website forms, cookie notices, marketing consents and unsubscribe processing.
- [ ] Train staff, trainers and contractors and retain attendance and acknowledgement records.
- [ ] Publish the approved policy and archive the superseded version.

Appendix 4 - Reference sources

Sources reviewed for this revision. These are external controlled sources and should be checked at each review. Accessed 13 July 2026.

Privacy Act 1988 - compilation in force 4 June 2026 - Official source
OAIC - Australian Privacy Principles - Official source
OAIC - Chapter 1, APP 1 open and transparent management - Official source
OAIC - Chapter 11, security of personal information - Official source
OAIC - Data breach preparation and response, Part 4 NDB scheme - Official source
ASQA - 2025 Standards for RTOs - Official source
Federal Register - 2025 Compliance Standards instrument - Official source
ASQA - Integrity of Nationally Recognised Training Practice Guide - Official source
Federal Register - Data Provision Requirements Instrument 2020 - Official source
Federal Register - Data Provision Requirements Amendment (Data Streamlining) Instrument 2026 - Official source
DEWR - VET activity data and transition pathways - Official source
DEWR - National VET Data Policy - Official source
DEWR - VET Data Privacy Notice - Official source
DEWR - Reporting requirements and data responsibilities under the VET Information Standard - Official source
DEWR - Guide to RTO Data Provision Requirements, 9 July 2026 - Official source
USI - Creating a USI on behalf of another person - Official source
USI - Giving access to your USI and VET transcript - Official source
ACMA - Avoid sending spam - Official source
CPR First Aid - current contact page - Official source

Approval

Approved by:

Position:

Signature:

Date: