



Privacy Policy

NNZMC Pty Ltd — Trading as Industry Skills Solutions

Registered Training Organisation #45974

VERSION 3.6 · JULY 2025 · RTO_POL_1.14

Document control

Version	Date	Author	Summary of change
2.0	02/03/2023	HM	Post-registration review
2.1	17/03/2023	KM	Updated complaints handling and concerns
3.0	07/2025	HM	Full review and update to align with the Standards for RTOs 2025 and current privacy law: references updated from the 2015 to the 2025 Standards; data-collection authority updated to the National VET Data Policy and AVETMISS; Privacy Act references updated to the 1988 Act as amended, including the Notifiable Data Breaches scheme; the 13 APPs, security, retention and access provisions reaffirmed.
3.1	07/2025	HM	Compliance review update: added a policy-availability statement and USI-handling section; expanded the data-breach response (roles, 30-day assessment, OAIC notification, documentation, plan location); added a differentiated retention schedule and specified the assessment-evidence period (2 years after completion of the training product); reconciled overseas disclosure with APP 8; added APP 12/13 refusal rights, identity verification, learner VET records access, prospective-learner data handling and sensitive-information consent (APP 3); described third-party obligations (APP 11); strengthened the privacy-complaints pathway with acknowledgement and resolution timeframes; added staff-awareness detail and update-notification; clarified operational ownership; standardised legislative citations; clarified the two-instrument Standards mapping; and aligned the cover, footer and control table to V3.1.
3.2	07/2025	HM	Further compliance review update: specified the minimum privacy information provided at/before enrolment (APP 5 — collector, purpose, likely disclosures to NCVER and government, access); added handling of records for learners who withdraw or do not complete; expanded third-party (APP 11) obligations and monitoring; added VET record-access parameters, RPL/credit-transfer information handling, third-party (employer/parent) access under APP 6, and data-migration/cessation provisions; added Federal Register instrument numbers (F2025L00354 and F2025L00355) to the Standards mapping so references can be verified.
3.3	07/2025	HM	Further review update: added inter-RTO record transfer, AVETMISS data-quality and correction of externally-reported data (APP 13), job-applicant handling, marketing-consent withdrawal (APP 7), the distinction between the 14-day APP timeframe and 24-hour training-record timeframe, complaints-record confidentiality, contractor-monitoring detail, confirmation the Data Breach Response Plan covers the NDB scheme, and complaint-delay notification.
3.4	07/2025	HM	Final review update (released version): added a defined retention entry for prospective-learner enquiry data; framed learner training-record access as a regulatory entitlement

Version	Date	Author	Summary of change
			(Compliance Standards s.10); added employer-contracted-training consent (APP 6), an AVETMISS use/disclosure limitation (National VET Data Policy), an access-request extension notice (APPs 12/13), an at-a-glance access-timeframe note, and a certification-information handling statement.
3.5	07/2025	HM	Compliance-manager review update: confirmed Industry Skills Solutions does not use personal information for direct marketing — removed “marketing” from the collection purposes, replaced the Direct Marketing section with a no-marketing statement, and removed the marketing-records retention row. Corrected the APP 5 collector identity to the full legal name (NNZMC Pty Ltd T/a Industry Skills Solutions, RTO 45974). Aligned the disclosure of results and Statements of Attainment to the actual operating model: for employer-funded or employer-commissioned training these are disclosed to that employer as a primary purpose, notified and consented to at enrolment (APP 5 and APP 6), while any other third-party disclosure still requires the learner’s written consent — the enrolment form and pre-enrolment privacy notice are to carry the corresponding consent, and the Issuing Certificates and Outcomes Policy is to be aligned. Renamed the privacy-complaint form to the single “Complaints and Appeals Form”.
3.6	07/2025	HM	Administrative update: standardised terminology to “Compliance Standards” to match the registered instrument title (the Compliance Standards Instrument 2025).

Operational owner	Compliance Manager (day-to-day administration of this policy)
Authorised by	Harrison McMahon, Chief Executive Officer
Next review	July 2027, or earlier if regulatory requirements change

Approved and released. Version 3.6 is the approved, current version of this Privacy Policy, released July 2025 and authorised by Harrison McMahon, Chief Executive Officer. No further changes are to be made except by issuing a new version.

Purpose and scope

NNZMC Pty Ltd T/a Industry Skills Solutions (Industry Skills Solutions) collects and stores personal information about learners, industry clients and staff. This policy sets out how we handle personal information in accordance with the Privacy Act 1988 (Cth), as amended — including the Australian Privacy Principles (APPs) in Schedule 1 and the Notifiable Data Breaches scheme — and with the Student Identifiers Act 2014 (Cth).

How this policy is made available

This policy is published on our website (www.industryskillssolutions.com.au), is provided to learners at enrolment through the Student Handbook, and is available on request. Our staff are directed to refer any privacy enquiry to this policy and to the Compliance Manager, so that prospective and current learners can readily locate and understand how their personal information is handled.

Definitions

- **Personal information** — information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether or not recorded in a material form.
- **Sensitive information** — includes racial or ethnic origin, political opinions or affiliations, religious or philosophical beliefs, professional or trade association or trade union membership, sexual orientation or practices, criminal record, and health, genetic and biometric information.

Authority to collect and store

Our authority to collect and store personal information derives from our registration by ASQA under the National Vocational Education and Training Regulator Act 2011 (Cth); our obligations under the Student Identifiers Act 2014 (Cth); our obligation to collect and report data in accordance with AVETMISS and the National VET Data Policy; the record-keeping requirements of the Standards for RTOs 2025; and our mandatory reporting obligations to government agencies.

Collection and use

We collect contact information (name, organisation, position, address, telephone, email) for delivery and support of training, mandatory reporting and stakeholder communication; training-related information such as satisfaction surveys, complaint-handling data and employer-client information per AVETMISS; and staff information for human-resource management. Collection methods include enrolment and administrative forms (paper or electronic), entry into our learner management system (aXcelerate), hard-copy learner files, employer and learner satisfaction surveys, and website enquiries.

We take reasonable steps to ensure the personal information we collect, use and report is accurate, complete and up to date. We are committed to reporting accurate and complete AVETMISS data to the NCVER in accordance with the National VET Data Policy, and if a reporting error is identified we correct our records and, where possible, notify the relevant body of the correction. Personal information collected for AVETMISS reporting is disclosed only to the NCVER and to Commonwealth and State or Territory training authorities as required under the National VET Data Policy, and is not used for any other purpose without your consent.

We also collect personal information from applicants for employment. Applicant information is used only to assess the application, is handled in accordance with this policy, and is retained only as long as needed — unsuccessful applicants' information is retained for up to 12 months and then securely destroyed (see our human-resources procedures for detail).

Sensitive information

Where required for national VET data collections and surveys (and VET-related research), we collect information such as disability or long-term impairment status, Indigenous status, language spoken at home, English proficiency and country of birth. We also collect dietary requirements for catering and, for staff, professional memberships and health or work-injury information for HR management. Consistent with APP 3, we collect sensitive information (such as disability and Indigenous status) with your consent — obtained at enrolment through the enrolment form — or where its collection is required or authorised by law (for example AVETMISS reporting), which we note to you at the point of collection.

Prospective learners

When you make a website enquiry or contact us before enrolling, we collect only the information needed to respond to your enquiry and to help you decide whether to enrol. If you do not proceed to enrol, we retain this information only for as long as needed for that purpose (and any follow-up you have agreed to) and then securely destroy or de-identify it.

Direct marketing

Industry Skills Solutions does not use your personal information for direct marketing. Communications we send you relate to your enrolment, training and assessment, our regulatory obligations, and learner and employer satisfaction surveys — these are operational communications, not marketing. We do not sell or rent personal information, and we do not cold-call for marketing purposes.

Website, analytics and cookies

Google Analytics collects cookies, including IP addresses, to compile web-usage reports; Google will not associate IP addresses with any other data it holds. You can disable cookies in your browser or opt out via Google's tool, though this may affect website functionality. Our web servers automatically log the server address, date, time and pages accessed for website management; no personal information is recorded in these logs.

Overseas processing (APP 8). Because Google Analytics processes some technical data (including IP addresses, which can be personal information) on servers located outside Australia, this involves a cross-border disclosure. We take reasonable steps to ensure it is handled consistently with Australian Privacy Principle 8, noting that Google is subject to comparable privacy protections. Apart from this limited technical data, we do not disclose personal information to overseas recipients.

Unique Student Identifier (USI)

We are required to collect and verify a Unique Student Identifier (USI) for every learner undertaking nationally recognised training, in accordance with the Student Identifiers Act 2014 (Cth). We use USIs only for the VET-related purposes permitted by that Act — for example issuing certification and reporting to the USI Registrar and the NCVER. USIs are stored securely in aXcelerate under the same access controls that apply to other personal information. We do not collect, use or disclose a USI except as authorised or required by the Student Identifiers Act 2014, and we do not include a learner's USI on their certification documentation. Personal information used to prepare and issue AQF certification (such as your full legal name and verified USI) is handled in accordance with this policy and the Student Identifiers Act 2014, and certification records are retained securely for 30 years.

Notification, disclosure and access

Notification of collection

We notify individuals at or before the time of collection (or as soon as practicable afterwards), usually in writing — for example on the course application page, in survey invitations, and on commencement of employment.

Before or at enrolment, we give learners the key privacy information required by APP 5: who is collecting the information (NNZMC Pty Ltd T/a Industry Skills Solutions, RTO 45974); the purposes of collection; that their information will be disclosed to the NCVER and to Commonwealth and State or Territory training authorities for statistical, regulatory and research purposes; and how to access or correct it. This information is set out in the privacy notice on our enrolment form and in the Student Handbook, so learners are informed before they commit to training.

Disclosure

We do not disclose personal information except for the purpose for which it was collected, with your consent for a secondary purpose, where you would reasonably expect it, or where required by law. We may share information with Commonwealth and State/Territory agencies and the NCVER in line with our contractual and reporting obligations, after taking reasonable steps to inform you and, where required, seek consent. Where you transfer to another RTO or seek recognition of your training, we make your training records (such as results and completion status) available to the receiving RTO or an authorised body with your consent, consistent with the records requirements of the Standards for RTOs 2025. Where

training is funded or commissioned by an employer or industry client, providing that employer with the learner's enrolment, progress, results and Statements of Attainment is a primary purpose of the training: the learner is notified of this, and gives their consent, at enrolment through the privacy notice on our enrolment form (APP 5 and APP 6). Our obligations to individual learners are not otherwise reduced. Any disclosure to a third party other than a funding or commissioning employer is made only with the learner's written consent, unless required by law (APP 6). We do not sell mailing lists. Other than the limited technical data described under "Website, analytics and cookies" above (handled consistently with APP 8), we do not disclose personal information to overseas recipients.

Access and correction

Subject to the exceptions in the APPs, you may request access to, and correction of, your personal information at no charge. Requests must be in writing, and we respond within 14 business days; if we cannot respond within that time, we will notify you of the delay and give you a revised timeframe (APPs 12 and 13). We may require reasonable proof of identity before acting on a request, to protect your information from unauthorised disclosure. If we refuse access or correction (in whole or in part), we will give you written reasons and advise you how to complain, including your right to complain to the OAIC (APPs 12 and 13). Where personal information has already been reported to the NCVET or a government authority, we correct our own records and, where possible, notify the relevant body of the correction.

Separately from these privacy rights, you also have a right — under the Compliance Standards of the Standards for RTOs 2025 (s.10) — to access your own training records, such as your results and completion status, at any time and at no charge, using the Student Records Request Form. This is a regulatory entitlement in addition to your rights under the APPs. We provide access as soon as possible and, in any case, within 24 hours (see the "Accessing your records" section of the Student Handbook).

At a glance — access timeframes. Formal privacy access or correction request (under the APPs): within 14 business days. Routine training-record request (results, completion status): within 24 hours.

We disclose a learner's personal information or training records to a third party other than a funding or commissioning employer — such as a non-funding employer, or the parent or guardian of a learner under 18 — only with the learner's written consent, or where required or authorised by law (APP 6). Such requests are handled through the same access process, including identity verification.

Information security, retention and disposal

We take active steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. Most data transferred over the internet is protected by Secure Sockets Layer (SSL); access to aXcelerate is controlled by user log-on, password and assigned access rights; premises and storage are secured, a clean-desk policy applies, and paper documents are locked or shredded and hardware sanitised before disposal. Third parties who handle personal information on our behalf — including contracted trainers and assessors, IT and software providers, and printing services — are located within Australia and are bound by appropriate privacy obligations through contractual terms or data-handling agreements, consistent with APP 11. These obligations require them to use personal information only for the purposes we specify, to maintain appropriate security, and to notify us immediately of any suspected breach; we confirm their compliance through our contract and vendor-management arrangements, including audit rights and periodic checks, and we require them to report any privacy incident to us. Data migration and system-transition activities (for example a change of learner management system) are subject to the same security and access controls as routine handling, and if we make a significant system change or cease to operate, records are managed in accordance with applicable regulatory requirements, including ASQA's requirements for the transfer of records.

Retention schedule

We retain records for the following minimum periods. Where more than one period could apply, we keep the record for the longer period. Information is securely destroyed or de-identified when no longer required and lawful to do so.

Record category	Minimum retention
Records of AQF certification issued (certification register)	30 years
Learner records and records of results	30 years
Completed assessment evidence	2 years after completion of the training product
Complaints and appeals records	5 years
Financial and transaction records	7 years
Staff and human-resource records	7 years after employment ends
Prospective-learner (pre-enrolment) enquiry data	Until no longer required for the enquiry, then destroyed

Records of learners who withdraw or do not complete are retained for the same minimum periods as those who complete — for example certification and results records for 30 years, and completed assessment evidence for 2 years. Personal information collected as part of a recognition of prior learning (RPL) or credit-transfer application — which can include prior qualifications, employment records and referee reports — is handled consistently with this policy (consent, security and retention), and RPL evidence is retained as assessment evidence (2 years after completion). Complaints and appeals records are handled confidentially and stored securely with restricted access, and are retained for the period shown above (see also the Complaints and Appeals Handling Policy). These periods are minimums and are confirmed against current legal and regulatory requirements.

Data breach response

We maintain a Data Breach Response Plan, which is available to staff from the Compliance Manager. If any worker becomes aware of, or suspects, a data breach — for example the loss of, or unauthorised access to or disclosure of, personal information — they must report it immediately to the Compliance Manager or CEO. We then act to contain the breach and assess whether it is an eligible data breach likely to result in serious harm, completing that assessment as quickly as possible and within 30 days, as required by the Notifiable Data Breaches scheme. Where a breach is likely to result in serious harm, the CEO or Compliance Manager notifies the affected individuals and the Office of the Australian Information Commissioner (OAIC) as soon as practicable. All breaches, assessments and actions taken are documented, and outcomes inform our continuous improvement. Our Data Breach Response Plan addresses all requirements of the Notifiable Data Breaches scheme, including the criteria for assessing the “serious harm” threshold and the notification pathways to affected individuals and the OAIC.

Privacy complaints and concerns

If you have a privacy concern, please raise it with a staff member, or lodge a Complaints and Appeals Form (available on our website or from our office) with the Compliance Manager at kerry@industryskillssolutions.com.au. We acknowledge privacy complaints within 2 business days, handle them confidentially, and aim to resolve them within 30 calendar days (and in any case within the 60-day maximum set out in our Complaints and Appeals Handling Policy), keeping you updated on progress. If we cannot resolve your complaint within 30 days, we notify you of the delay and give you a revised expected resolution date. If you are not satisfied with our response, you may complain to the OAIC at oaic.gov.au/privacy/privacy-complaints or on 1300 363 992.

Staff awareness and review

Privacy awareness is a documented component of staff induction, with a sign-off record, and is reinforced through refresher activities at least annually. Contractors who have access to personal information (including trainers, assessors and IT providers) receive an equivalent briefing and are bound by contractual privacy obligations. When this policy is updated, staff are notified (for example by email or at a team meeting) and are required to acknowledge the updated version.

We monitor developments in privacy law and update this policy as required; the current version is always available on our website. Privacy information provided to learners (in the Student Handbook and on enrolment forms) is reviewed whenever this policy is updated, and learners are notified of any material change that affects how their information is handled. This policy is reviewed at least every two years, or earlier if regulatory requirements change.

Mapping to the Standards for RTOs 2025

The Standards for RTOs 2025 comprise two instruments on the Federal Register: the Outcome Standards Instrument 2025 (F2025L00354), which contains the Outcome Standards (Standards 1.1–4.4, grouped into four Quality Areas); and the Compliance Standards Instrument 2025 (F2025L00355), which contains the Compliance Standards (numbered sections s.7–s.20). This policy is cross-referenced to both — only the standards and requirements it addresses are listed, with the section of this document that addresses each.

Standard or requirement	What it requires	Addressed in this policy
Outcome Standard 2.1 — Access to information about the organisation	Clear, accurate information about the RTO and how it handles personal information is accessible before and during enrolment.	Purpose and scope; How this policy is made available; Notification, disclosure and access
Outcome Standard 2.7 — Feedback and complaints	An accessible, fair process addresses privacy concerns and informs improvement.	Privacy complaints and concerns
Outcome Standard 4.3 — Risk management	Risks to students, staff and the organisation — including to personal information — are identified and managed.	Information security, retention and disposal; Data breach response
Compliance Standards 2025, s.20 — Compliance with laws	Personal information is handled in accordance with privacy law and the Student Identifiers Act 2014.	Purpose and scope; Authority to collect and store; Unique Student Identifier (USI)
Compliance Standards 2025, s.10 — Records	Certification and assessment records are retained and accessible.	Information security, retention and disposal (retention schedule)
Compliance Standards 2025, s.12 — Student identifier	USIs are collected, verified, used and disclosed only as permitted under the Student Identifiers Act 2014.	Unique Student Identifier (USI)

Related documents and legislation

This policy should be read together with: the Student Handbook, the Complaints and Appeals Handling Policy, and our records-management and data-breach procedures; and the Privacy Act 1988 (Cth), the National Vocational Education and Training Regulator Act 2011 (Cth), the Student Identifiers Act 2014 (Cth), the Spam Act 2003 (Cth) and the Do Not Call Register Act 2006 (Cth).

Authorisation

This policy is authorised by the Chief Executive Officer of NNZMC Pty Ltd T/a Industry Skills Solutions.

Name	Harrison McMahon
Position	Chief Executive Officer
Signature	
Date	01/07/2025