Confidentiality, Privacy and Information Security Policy

Establishes proportionate protection for personal, commercial, QMS, technical and restricted examination information.

Status	Rev 0 - initial issue	**Effective date**	15/09/2026
Classification	Controlled QMS policy	**Process owner**	As assigned in this document

Contents

1. Purpose and Scope 2
2. Policy commitments 2
3. Abbreviations & Definitions 2
4. Responsibilities 3
5. Privacy information lifecycle 4
   5.1 Collection and notice 4
   5.2 Sensitive information 4
   5.3 Use and disclosure 4
   5.4 Consent and authorised disclosure 5
   5.5 Learner identifiers 5
   5.6 Storage and security 5
   5.7 Access and correction 5
   5.8 Privacy incidents and notifiable breaches 5
   5.9 Electronic communication 5
   5.10 Confidentiality 5
   5.11 Retention and secure disposal 6
   5.12 Privacy complaints 6
6. Implementation and review 6
7. Certification Body controls 6
8. Controlled references and records 7
   9.1 Revision Table 7
   9.2 Revision Comments 7

1. Purpose and Scope

This policy establishes proportionate protection for personal, commercial, QMS, technical and restricted examination information and controls personal information throughout its collection, use, disclosure, storage, retention and disposal.

It applies to information in any format, location or system, including paper, electronic, image, audio, portable media, cloud services and remote or external locations.

The policy applies to personal information about prospective, current and former learners and candidates; staff; trainers; assessors; examiners; contractors; consultants; employers and workplace representatives; service providers; visitors; and any other person whose information is collected or managed by QMTS Industry Training.

It applies to all QMTS Industry Training personnel and service providers who collect, access, use, disclose, store, transport, retain or dispose of information for an authorised purpose.

2. Policy commitments

QMTS Industry Training shall:

- Classify information as Public, Internal, Confidential or Restricted Examination and apply handling controls accordingly;
- Limit access to authorised roles with a current business need and periodically review permissions;
- Segregate formal qualification-examination material from training material;
- Collect only the personal and sensitive information necessary for legitimate business, training, assessment, certification, regulatory and contractual purposes;
- Provide clear collection notices explaining why information is collected, how it will be used or disclosed, and how access, correction and complaints are handled;
- Use and disclose personal information only for the purpose of collection, a reasonably expected related purpose, with valid consent, or where authorised or required by law;
- Protect personal and sensitive information from misuse, interference, loss, unauthorised access, modification or disclosure;
- Provide reasonable access to personal information and correct information that is inaccurate, incomplete, out of date, irrelevant or misleading, subject to lawful exceptions;
- Protect integrity, availability, backup and recoverability as well as confidentiality;
- Retain and securely dispose of information in accordance with applicable legal, regulatory, contractual and CB requirements;
- Report and respond to suspected loss, disclosure, alteration, cyber events, privacy breaches or examination compromise immediately.

3. Abbreviations & Definitions

Term / abbreviation	Definition
QMS	Quality Management System
CB / CBs	Certification Body / Certification Bodies
BINDT	British Institute of Non-Destructive Testing
AINDT	Australian Institute for Non-Destructive Testing
PCN24	BINDT's PCN24 certification scheme and document series
AQB	Authorised Qualifying Body

Term / abbreviation	Definition
NCR	Nonconformance Record
Cth	Commonwealth of Australia
RTO	Registered Training Organisation
APP / APPs	Australian Privacy Principle / Australian Privacy Principles
NDB	Notifiable Data Breaches scheme under the Privacy Act 1988 (Cth)
USI / USIs	Unique Student Identifier / Unique Student Identifiers
VET	Vocational Education and Training
NCVER	National Centre for Vocational Education Research
OAIC	Office of the Australian Information Commissioner
AQF	Australian Qualifications Framework
SMS	Student Management System
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable.
Sensitive information	Personal information requiring additional protection, including health, disability and other categories treated as sensitive under applicable law.
Privacy breach	Loss, unauthorised access, unauthorised disclosure, alteration or misuse of personal information.
Restricted Examination	Examination questions, answers, specimens, marking material, master reports, results and related controlled information requiring the highest handling controls.

4. Responsibilities

Role	Policy responsibility
QMS Manager	Owns this policy, information classification, privacy compliance monitoring, access and correction requests, privacy complaints, authorised disclosure decisions, breach records and incident coordination.
Chief Examiner	Owns restricted examination security and segregation, protects candidate and examination records, limits disclosure to authorised purposes and reports suspected compromise immediately.
System owner	Implements approved access, secure storage, backup, logging, recovery and cybersecurity controls and supports the containment and investigation of information incidents.
Training and examination personnel	Protect learner and candidate personal, sensitive and assessment information, access it only for authorised duties and report suspected loss or disclosure immediately.

Role	Policy responsibility
All users	Use information only for authorised purposes and protect credentials, screens, printouts, devices, conversations and information in transit.
Learners and candidates	Provide accurate information, advise relevant changes, protect their account credentials and respect the privacy and confidentiality of other people.

5. Privacy information lifecycle

5.1 Collection and notice

QMTS Industry Training collects personal information only where it is reasonably necessary for its functions or activities. Collection may support enrolment and identity verification; eligibility and funding decisions; USI administration; learner or candidate support; training, examination and assessment; attendance and achievement records; AQF certification; complaints and appeals; communications; quality assurance; and legal, regulatory, contractual or CB reporting.

At or before collection, or as soon as practicable afterwards, the individual is given a clear notice describing the purpose of collection, the expected uses and disclosures, any usual recipients, the consequences of not providing required information, and how to request access or correction or make a privacy complaint.

Information collected may include identity and contact details, emergency contacts, eligibility and prior-qualification information, USIs and verification documents, enrolment and support information, attendance, assessment evidence and outcomes, employment and workplace information, funding details, payment or invoicing information, and communication records.

5.2 Sensitive information

Sensitive information is collected only where necessary and with consent or another lawful authority. It may include disability or health information relevant to safe participation, assessment or workplace requirements; cultural or language considerations; and information needed to identify and implement reasonable adjustments or learner support.

Sensitive information is used and disclosed only for the purpose for which it was provided or as otherwise authorised or required by law. Access is limited to personnel who need the information to perform an authorised duty.

5.3 Use and disclosure

Personal information is used or disclosed for the purpose for which it was collected, a related purpose the individual would reasonably expect, with valid consent, or where authorised or required by law. Relevant uses include learner and candidate administration, training and assessment, certification, government and CB reporting, quality assurance, auditing, compliance monitoring and service communication.

Authorised recipients may include applicable CBs and AQBs; the applicable VET regulator; NCVER; the Student Identifiers Registrar; Commonwealth, State or Territory agencies; funding authorities; employers or workplace representatives where authorised; approved auditors and assessors; and contracted service providers supporting administration, records or information systems.

Before release, QMTS IT verifies the recipient, purpose and authority. Service providers must be subject to contractual or other reasonable controls requiring secure handling and compliance with applicable privacy obligations.

5.4 Consent and authorised disclosure

Where consent is required, it must be voluntary, informed, current and specific to the intended purpose. QMTS IT explains the proposed disclosure and recipient, records the consent where appropriate and permits withdrawal where legally and practically possible. Withdrawal may affect service delivery or the ability to meet a regulatory obligation.

Additional consent is not required where collection, use or disclosure is authorised or required by law or is otherwise permitted, including required VET, USI, funding, court, law-enforcement, health or safety, regulator or CB reporting. The basis for a material disclosure is recorded.

5.5 Learner identifiers

Where RTO or VET activities require a USI, QMTS IT collects and verifies the USI, protects it from misuse and unauthorised access or disclosure, and uses it only for an authorised purpose. Identity information collected solely to apply for a USI is securely destroyed as soon as practicable after it is no longer needed for that purpose.

5.6 Storage and security

Personal and confidential information is protected through approved repositories, password and multi-factor controls where configured, least-privilege access, access reviews, logging, secure cloud services, locked storage for paper records, protected transport, backups, recovery testing, current malware and cybersecurity controls, and authorised destruction.

Access is attributable and removed promptly when duties end or change. Information must not be stored in unapproved locations, sent through an unapproved channel or left visible or accessible to an unauthorised person.

5.7 Access and correction

An individual may request access to personal information held about them or ask for correction where it is inaccurate, incomplete, out of date, irrelevant or misleading. QMTS IT verifies identity, responds within a reasonable timeframe and records the request and outcome.

Where access or correction cannot lawfully be provided, QMTS IT explains the decision and available review or complaint route, unless giving the reason would itself be unlawful or unreasonable.

5.8 Privacy incidents and notifiable breaches

Any actual or suspected privacy breach must be reported immediately to the QMS Manager. QMTS IT contains the incident, preserves relevant evidence, assesses affected information and likely harm, documents decisions, coordinates remediation and records corrective action through the applicable incident or NCR process.

Where the NDB scheme applies, QMTS IT undertakes an expeditious assessment, taking reasonable steps to complete it within the statutory assessment period, and notifies the OAIC and affected individuals when an eligible data breach is established. Relevant regulators and CBs are also notified where their requirements apply.

5.9 Electronic communication

QMTS Industry Training may communicate through email, text message, telephone, an approved Student Management System (SMS), a learning management system or another approved platform. Reasonable safeguards are applied to the sensitivity of the information, including recipient verification, restricted attachments or links, access controls and secure transmission where required.

5.10 Confidentiality

Personnel must maintain the confidentiality of learner and candidate records, assessment and examination outcomes, complaints and appeals, employment records, financial information, commercially sensitive information

and Restricted Examination material. Unauthorised access, use or disclosure may result in disciplinary or contractual action and legal, regulatory or CB escalation.

5.11 Retention and secure disposal

Records are retained under QMTS-QA-PR-003 and any longer legal, regulatory, contractual or CB requirement. Where the 2025 RTO Compliance Standards apply, records of AQF certification documentation issued to VET students are retained for 30 years and assessment evidence submitted by a VET student is retained for two years after completion of the training product, unless another requirement is longer.

At the end of the applicable retention period, information no longer required is securely destroyed or permanently de-identified. Disposal is authorised, protects confidentiality and is recorded where evidence of destruction is required.

5.12 Privacy complaints

An individual may make a privacy complaint if they believe their personal information has been mishandled. The complaint is acknowledged promptly, investigated fairly, handled confidentially and resolved within a reasonable timeframe under QMTS-QA-PL-004.

If the individual remains dissatisfied, QMTS IT explains any available external review route, including the OAIC or the applicable regulator where relevant.

6. Implementation and review

Access is approved, attributable, least-privilege and removed promptly when duties end or change.

Restricted examination records use controlled repositories, secure transport, issue and return reconciliation and authorised disposal.

External disclosure occurs only with authority, lawful basis or a current CB requirement; identity is verified before release.

Information incidents are contained, preserved, risk assessed, investigated and notified to affected parties, regulators or CBs where required.

Personnel receive information and guidance appropriate to their role and must understand the privacy, confidentiality and information-security controls that apply to their work.

This policy is reviewed at intervals not exceeding three years and earlier when legal, regulatory, contractual or CB requirements change, or when an incident, audit or management review identifies a need.

7. Certification Body controls

Applicability	Required control
All CBs	Protect examination questions, answers, specimens, master reports, marking material, results and candidate records from unauthorised access or disclosure.
BINDT only	Apply current PCN24 AQB security, remote-location, custody and BINDT access or notification requirements.
AINDT only	Apply current AINDT AQB confidentiality, examiner or invigilator and examination-material controls.

8. Controlled references and records

Type	Controlled source / objective evidence
External - privacy	Privacy Act 1988 (Cth) and the APPs, including the NDB scheme, where applicable.
External - learner identifiers	Student Identifiers Act 2014 (Cth), where RTO or USI activities apply.
External - VET and RTO	2025 Standards for RTOs and applicable 2025 Compliance Standards; National VET Data Policy and current provider data standard; AQF Qualifications Register Policy, where applicable.
External - certification	Current applicable CB security, confidentiality, custody, access and notification requirements.
Internal	QMTS-QA-PL-004; QMTS-QA-PR-003; QMTS-QA-PR-018; QMTS-QA-FR-029; QMTS-QA-FR-031.
Records	Collection notices; consent and disclosure-authority records; access and correction requests; privacy complaints; privacy-breach, incident and NCR records; access authorisations; material-movement and secure-disposal records.
External - named source	PCN24: current applicable security, remote-location, custody and access or notification requirements.
Internal - referenced register	Controlled external-document register (document number not stated in this policy).

External references are not reproduced by this document. The controlled external-document register identifies the current issue, owner, review date, change assessment and transition action.

9.1 Revision Table

Rev.	Date	Originator	Reviewer	Details
0	15/09/2026	Michael Taylor	Dean Mallaburn	Approved for use – Commercial Director

9.2 Revision Comments