Policy area	Governance
Standards	Compliance Standards for RTOs 2025, Standard20
Responsibility	CEO, Office Manager

1. Introduction and Purpose

The Privacy Protection Policy of Heaton Institute of Technology establishes a framework for managing personal information in compliance with the Australian Privacy Act 1988 and the Australian Privacy Principles (APPs). The policy aims to:

- Ensure lawful collection, use, storage, and disclosure of personal information.
- Protect personal and sensitive information from misuse, loss, unauthorized access, or disclosure.
- Provide strategies for securing both physical and digital information.
- Establish an information classification system to control access, distribution, and handling of information.

The policy applies to students, staff, clients, and other stakeholders whose personal information is collected and managed by the institute.

2. Definitions of Personal, Sensitive and Credit Information

Personal Information

Personal information refers to any information that identifies or can reasonably identify an individual. Examples include:

- Name, address, phone number, and date of birth
- Employee records
- Photographs
- IP addresses
- Biometric data (facial recognition, voice prints)
- Location data from mobile devices

The policy also recognizes "high-risk personal information" such as:

- Passport details
- Driver’s licence information
- Medicare details
- Birth certificates
- Visa documentation

These documents create a heightened risk of identity theft if compromised.

Sensitive Information

Sensitive information includes data relating to:

- Health information
- Racial or ethnic origin
- Religious beliefs
- Political opinions
- Trade union membership
- Criminal records
- Genetic and biometric information

Credit Information

Credit information includes personal and financial details used to assess an individual's creditworthiness, such as repayment history, defaults, insolvency records, and credit applications.

3. Privacy Commitment and Legal Authority

Heaton Institute of Technology collects and stores personal and sensitive information to meet legislative and operational requirements.

The policy recognizes that privacy breaches can result in:

- Financial loss
- Reputational damage
- Loss of student and business confidence
- Operational disruption

Strong privacy practices reduce the likelihood of breaches while improving efficiency and compliance.

Legal Authority for Collection

The institute is legally required to collect information under:

- National Vocational Education and Training Regulator Act 2011
- Data Provision Requirements 2020
- Australian Vocational Education and Training Information Statistical Standard (AVETMISS)
- Student Identifiers Act 2014

These laws require the collection, retention, and reporting of student information, including Unique Student Identifier (USI) verification data. Student records may need to be retained for up to 30 years.

4. Collection and Use of Personal Information Purpose

The institute uses personal information for:

- Student enrolment and administration
- Government reporting requirements
- Licensing and certification processes
- Satisfaction surveys
- Complaint management
- Marketing and communication activities
- Human resource management

Information collected may include:

- Contact details
- Emergency contacts
- Employment records
- Banking information for staff

Students are informed about privacy practices through the Student Handbook and National VET Data Policy.

Sensitive Information Collection

Examples include:

- Disability and health-related information
- Indigenous status
- Language and country of birth data
- Dietary requirements for events
- Professional memberships
- Employee health and injury records

These are collected only when necessary for training, compliance, or operational purposes.

5. Marketing, Unsolicited Information and Notifications

Direct Marketing

The institute complies with:

- Australian Privacy Principle 7
- Spam Act 2003
- Do Not Call Register Act 2006

Key principles include:

- Providing unsubscribes options
- Avoiding unsolicited marketing
- Prohibiting cold-calling practices

Unsolicited Personal Information

When personal information is received without being requested:

1. The institute evaluates whether it could legally collect the information.
2. Determines whether it is necessary for operations.
3. If unnecessary, the information must be destroyed or de-identified promptly.

Example:
If a parent sends medical information about an adult student without request, the institute must assess and usually destroy or de-identify the information.

Notification of Collection

Individuals are informed when information is collected through:

- Website privacy notices
- Student handbooks
- Survey invitations
- Employment commencement documentation

6. Disclosure, Access and High-Risk Information Management

Disclosure of Personal Information

Information may only be disclosed when:

- Required for the original purpose of collection
- Consent has been obtained
- Required by law
- Reasonably expected by the individual

The institute:

- Does not sell mailing lists
- Does not distribute student contact information
- Does not disclose information to overseas recipients

Access and Correction Rights

Individuals may:

- Request access to their personal information
- Request corrections to inaccurate records

Access is generally provided without charge, except for certain administrative costs associated with producing copies.

High-Risk Information

Copies of passports, licences, and similar identification documents must be:

- Destroyed after verification is completed
- Avoided whenever possible through direct verification
- Replaced with verification records documenting:
  - Type of document viewed
  - Date viewed
  - Staff member conducting verification

This minimizes identity theft risks.

7. Student Images and Physical Information Security

Student Images

Photographs and videos are considered personal information.

Students Under 18

- Images cannot be used for marketing, advertising, or promotional purposes.
- This restriction applies even with parental consent.

Students Aged 18 and Over

- Consent is obtained through enrolment processes.
- Students may opt out by notifying the institute in writing.

All images must be:

- Securely stored
- Used only for authorized purposes
- Protected under privacy requirements

Misuse of images constitutes a serious breach of policy and may result in disciplinary action.

Hard-Copy Information Security

Security measures include:

- Locked storage cabinets and rooms
- Restricted key distribution
- Proper file labelling and organization
- Secure document shredding
- Staff training
- Visitor supervision

- Monthly access audits
- Digitisation and backups
- Clean desk requirements

8. Digital Security and Information Classification

Digital Information Security

The institute requires:

Access Controls

- Unique user accounts
- Strong passwords
- Multi-factor authentication (MFA)

Cloud Security

Approved services include:

- Microsoft 365
- Dropbox
- Google Drive

Access permissions must be role-based and regularly reviewed.

Device Protection

- Automatic updates
- Antivirus software
- Firewalls

Data Protection

- Encryption of sensitive information
- Regular backups
- Disaster recovery capability within 24 hours

Remote Work Security

- Secure use of Teams and Zoom
- VPN uses on public networks

Staff Training

Annual cybersecurity awareness training covering:

- Phishing attacks
- Password security
- Handling sensitive information

Website Security

- SSL certificates
- Security plugins
- Restricted administrator access
- Regular updates and backups

Information Classification Labels

The policy establishes eight information categories:

Classification	*Purpose*
Public	Information openly available
Internal Only	Internal operational documents
Academic	Training and assessment materials
Confidential	Business-sensitive information
Restricted	Highly sensitive business information
Private	Personal and student records
Critical	Essential business continuity information
Regulatory	Compliance and legal records

Each classification has specific requirements for access, storage, transmission, and disclosure to ensure information is handled appropriately and securely.

Conclusion

The Privacy Protection Policy establishes a comprehensive framework for privacy compliance, information security, risk management, and regulatory obligations. It ensures that personal and sensitive information is collected, stored, used, disclosed, and destroyed responsibly while protecting the interests of students, staff, and the organization.