

Policy Statement

Heed Health Education (HHE) respects the privacy of students, prospective students, graduates, staff, contractors, clients, placement participants and other people who interact with us. HHE manages personal information openly, lawfully and securely and only collects, uses and discloses information where it is reasonably necessary for our education, training, assessment, student support, regulatory and business functions.

HHE is committed to complying with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Notifiable Data Breaches scheme and privacy requirements that apply to registered training organisations and VET Student Loans providers.

Purpose

This policy explains:

- the kinds of personal and sensitive information HHE collects and holds
- how HHE collects, uses, stores and discloses that information
- when information may be shared with government agencies, regulators, service providers and placement partners
- how individuals may access or correct their information
- how privacy concerns and eligible data breaches are managed.

Scope

This policy applies to personal information handled by HHE in paper and electronic records, websites, online forms, student management and learning systems, email, telephone and video communications, practical training, assessment and clinical placement activities. It applies to HHE employees, trainers, assessors, contractors and authorised service providers.

Government agencies, regulators and third parties that receive information from HHE manage that information under their own privacy obligations and policies.

Key Definitions

Term	Meaning
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable.
Sensitive information	A category of personal information that includes health information and information about racial or ethnic origin, religious beliefs, sexual orientation, criminal record, disability and professional or trade association membership.
Health information	Information or an opinion about a person's health, disability, injury or health services provided to them.
Data breach	Unauthorised access to, disclosure of, or loss of personal information held by HHE.

Information we Collect and Hold

Depending on the person's relationship with HHE, we may collect and hold:

- identity and contact details, including name, date of birth, address, email, telephone number and emergency contact details
- enrolment and demographic information required for AVETMISS and government reporting, including language, education, employment, disability and cultural background information
- Unique Student Identifier (USI), identity verification information and, where authorised, information needed to create, locate or verify a USI
- citizenship, residency and eligibility evidence; VET Student Loans information; Commonwealth Higher Education Student Support Number (CHESSN); tax file number information submitted through approved government processes; and loan-related records
- course participation, attendance, progress, assessment evidence, results, feedback, complaints, appeals, support plans, reasonable adjustment and academic integrity records
- health, disability, injury, medication, dietary or access information where needed to support safe participation, reasonable adjustment, practical training or clinical placement
- clinical placement documentation, clearances, licences, immunisation or screening evidence where required by HHE or a placement host
- images, audio, video, online-proctoring information, webinar recordings and practical assessment recordings where notified and reasonably required
- payment, invoicing and transaction details (HHE does not intentionally retain complete card details where payment is processed by a payment provider)
- website and systems data such as IP address, device/browser information, cookies, login records and system activity
- communications and enquiries, survey responses, marketing preferences and records relating to prospective students, clients, employees, applicants and contractors.

Where HHE does not need to identify an individual, a person may deal with us anonymously or using a pseudonym. This may not be practicable where identity is required for enrolment, assessment, certification, VET Student Loans, USI, placement, safety, contractual or legal purposes.

How we Collect Information

HHE usually collects information directly from the individual, including through enquiries, applications, enrolment and VET Student Loans processes, forms, assessments, surveys, telephone calls, email, websites, the student management system, learning management system, practical workshops and clinical placement.

We may also collect information from an authorised representative, parent or guardian, employer or client, previous training provider, government agency, USI Registry, funding body, placement host, referee, public source or service provider where the individual has consented, would reasonably expect the collection, or collection is authorised or required by law.

If HHE receives unsolicited personal information, we will assess whether we could have lawfully collected it. If not, and where lawful and reasonable, we will destroy or de-identify it.

Why we Collect, Use and Disclose Information

HHE may use and disclose personal information to:

- respond to enquiries and assess applications, eligibility, enrolment and credit transfer or recognition of prior learning requests
- deliver training, assessment, student support, reasonable adjustment, certification and clinical placement activities
- administer fees, refunds, VET Student Loans, census day requirements, electronic Commonwealth Assistance Forms, Commonwealth Assistance Notices and related reporting
- verify identity, obtain or verify a USI where authorised, and issue nationally recognised certification
- monitor participation, academic progress, quality, safety, wellbeing, complaints, appeals and compliance
- communicate with students, authorised representatives, employers or clients and provide course or service updates
- meet contractual, insurance, audit, recordkeeping, reporting and legal obligations
- improve HHE courses, services, systems and student outcomes through surveys, validation, analysis and quality assurance
- protect HHE, its community and the public from fraud, misconduct, cyber threats and health or safety risks.

HHE will not use or disclose personal information for an unrelated purpose unless the individual has consented or the use or disclosure is otherwise permitted or required by law.

Required VET, USI and VET Student Loans Disclosures

As an RTO, HHE is required to collect and report information under the National Vocational Education and Training Regulator Act 2011, the Data Provision Requirements, the National VET Data Policy and associated standards. Student information may be disclosed to the National Centre for Vocational Education Research (NCVER), Commonwealth and state or territory government departments, training authorities, funding bodies and the Australian Skills Quality Authority (ASQA).

Information disclosed to NCVER and authorised agencies may be used for authenticated VET transcripts, VET administration, regulation, monitoring, evaluation, research, statistics, surveys, data linkage, policy development, workforce planning and consumer information. Students may be contacted for a government or NCVER survey and may opt out when contacted where that option is offered.

For students applying for or accessing a VET Student Loan, HHE may collect, use and disclose VET information as authorised by the VET Student Loans Act 2016, the VET Student Loans Rules 2016 and related law. Information may be disclosed to the responsible Australian Government department, the Australian Taxation Office and other authorised bodies for eligibility, loan administration, compliance, review and debt purposes.

HHE will obtain permission where required before creating, locating or accessing a student's USI or viewing or sharing a USI VET transcript. The Student Identifiers Registrar separately manages USI information under the Student Identifiers Act 2014 and the Privacy Act 1988.

Other Disclosures and Services Provided

HHE may disclose relevant information to:

- Medical Edge Australia, as HHE's owner and primary clinical placement partner, where required for governance, shared services, student support, operational coordination, placement, safety or compliance
- approved clinical placement hosts, employers and clients, limited to information reasonably required to arrange, supervise and assess training or placement and manage safety
- technology, cloud hosting, student management, learning management, communications, payment, IT support, document storage, survey, identity verification and professional service providers
- auditors, insurers, legal advisers, accountants, regulators, courts, tribunals, law enforcement or emergency services where authorised or required
- a parent, guardian, authorised representative or other person where valid authority or consent has been provided, or where otherwise permitted by law.

HHE requires staff and service providers to access only the information needed for their role and to handle it confidentially and securely.

Overseas Disclosure and Cloud Services

Some technology or cloud service providers may store, process, back up or support information outside Australia. The countries involved may vary according to the provider and its service arrangements. Before using providers that may involve overseas disclosure, HHE takes reasonable steps to assess privacy and security safeguards and, where APP 8 applies, to ensure overseas recipients handle personal information consistently with the APPs unless an exception applies. Further information about current providers or likely locations may be requested from HHE's Privacy Officer.

Direct Marketing

HHE may use contact details to provide information about courses, services or events where consent has been given, or direct marketing is otherwise permitted by law. HHE does not sell personal information. Every electronic marketing message will provide a practical way to unsubscribe. Individuals may opt out at any time by using the unsubscribe function or contacting HHE. Opting out of marketing does not prevent HHE from sending essential enrolment, course, safety, compliance or service communications.

Website, Cookies and Analytics

HHE's website and online services may use cookies, server logs and analytics tools to operate securely, remember preferences, understand usage and improve content and performance. Information may include device, browser, IP address, pages viewed, referring website and approximate location. Browser settings may be used to manage cookies, although disabling them may affect site functionality. Third-party websites linked from HHE's website have their own privacy practices.

Security, Storage and Retention

HHE takes reasonable physical, administrative and technical steps to protect information from misuse, interference, loss and unauthorised access, modification or disclosure. Controls may include role-based access, passwords and multi-factor authentication, secure systems and backups, encryption where appropriate, staff confidentiality obligations, training, access review, vendor due diligence and secure disposal.

Records may be stored electronically or in hard copy. HHE retains training, assessment, certification, VET Student Loans, financial and other records for the periods required by applicable law, regulatory standards, funding contracts and legitimate business needs. When information is no longer required, and HHE is not legally required to retain it, HHE will take reasonable steps to securely destroy or de-identify it.

Accuracy, Access and Correction

HHE takes reasonable steps to keep personal information accurate, complete, relevant and current. Individuals should advise HHE when their details change.

An individual may request access to, or correction of, personal information HHE holds about them by contacting the Privacy Officer. HHE may need to verify identity and clarify the request. HHE will respond within a reasonable period and will not charge for making a request. Access may be refused or limited where permitted by law; if so, HHE will provide written reasons and available complaint options where required. If HHE declines to make a requested correction, the individual may ask HHE to associate a statement with the record.

Privacy Incidents and Data Breaches

Suspected loss, unauthorised access or disclosure of personal information must be reported promptly to HHE's Privacy Officer. HHE will contain and assess the incident, take remedial action and document its response. Where HHE has reasonable grounds to believe an eligible data breach is likely to result in serious harm, HHE will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as required by the Notifiable Data Breaches scheme.

Privacy Complaints

A person who believes HHE has mishandled their personal information should submit the concern to the Privacy Officer and include enough detail for HHE to investigate. HHE will acknowledge the complaint, investigate it confidentially and provide a written outcome within a reasonable period. HHE aims to respond within 30 calendar days; if more time is required, HHE will explain the reason and provide an updated timeframe.

If the person is not satisfied with HHE's response, they may use HHE's Complaints and Appeals process and/or contact the OAIC. The OAIC generally expects a person to first give the organisation an opportunity to respond.

Contact Details

Privacy contact	General Manager
Organisation	Heed Health Education (HHE)
Email	manager@heededucation.edu.au
Website	www.heedhealtheducation.com.au
External regulator	Office of the Australian Information Commissioner — www.oaic.gov.au 1300 363 992

Responsibilities

- The CEO and General Manager are responsible for organisational oversight and adequate privacy governance.
- The Privacy Officer coordinates privacy enquiries, access and correction requests, complaints and data breach assessment.
- Managers ensure privacy controls are applied within their functions and that service providers are appropriately managed.
- All staff, trainers, assessors and contractors must comply with this policy, protect credentials, limit access to a genuine work need and report suspected incidents immediately.

Related Legislation and Documents

- Privacy Act 1988 (Cth) and Australian Privacy Principles
- Notifiable Data Breaches scheme (Privacy Act 1988, Part IIIC)
- National Vocational Education and Training Regulator Act 2011 (Cth)
- Data Provision Requirements and National VET Data Policy
- Student Identifiers Act 2014 (Cth)
- VET Student Loans Act 2016 (Cth) and VET Student Loans Rules 2016
- HHE Complaints and Appeals Policy and Procedure
- HHE Records Management, Information Security and Data Breach Response procedures (where applicable).

Review and Publication

This policy will be reviewed at least annually and earlier where legislation, regulatory guidance, technology, systems or HHE operations materially change. The current version will be made available on HHE's website and through relevant student information channels.

Document History

Version	Date	Summary of changes	Approved by
1.3	Previous	Previous HHE Privacy Policy	HHE
2.0	6 th October 2025	Comprehensive rewrite for current HHE RTO, digital delivery, clinical placement and VSL operations; updated privacy and data breach provisions.	CEO / General Manager

Document Control

Document Number	007
Version	2.0
Effective Date	6 th October 2025
Policy Owner	General Manager / Privacy Officer
Next Review	October 2026, or earlier if legislation or operations change